SFN3300 Series

User Guide

Version 2.2

Contents

1 Preface

Copyright

The information in this document is subject to change without notice. In no event shall Sofinet be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this manual or the related content on the website, even if advised of the possibility of such damage.

Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

Manual Introduction

This manual introduces all the software functions supported by SFN3300 series switch, including function configurations and monitoring and maintaining, and provides typical configuration cases.

This manual instructs the readers to use the configurations by cooperating with SFN3300 *Series Switch Command Manual.*

Product Versions

The corresponding product versions of the manual are as follows:

Product Name	Product Version
SFN3300 Series switch	SOFOS SFN3300-24T4X (V1) SOFOS SFN3300-48T4X (V1) SOFOS SFN3300-24P4X (V1) SOFOS SFN3300-48P4X (V1)

Audience

This documentation is intended for:

- Commissioning engineers
- Field maintenance engineers
- System maintenance engineers

Conventions

Conventions of screen output format:

Format	Description
Screen print	Represents the output information of the screen
Keywords of Screen print	The red part represents the key information in the screen output

Conventions:

Format	Description
 Note	An alert that contains additional or supplementary information.
 Caution	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.

Format	Description
	An alert that calls attention to important information that if not understood or followed can result in personal injury or device damage.

Command conventions:

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
Italic	Italic text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

The icons used in the manual and the meanings:

Icon	Description
	Represents a generic switch
	Represents a generic router

Supporting Manuals of Product

Manual name	Overview
SOFOS SFN3300 Series Switch Installation Manual	Describes the device hardware specifications and installation methods, guiding you to install the device
SOFOS SFN3300 Series Switch Command Manual	Describes the device commands, equivalent to command dictionary, convenient for searching for the function of each command

Obtaining Documentation

You can access the most up-to-date SOFINET product documentation on the World Wide Web at www.sofinet.ru.

Technical Support

- Technical supporting hotline: 8(800)302-05-57
- Email: support@sofinet.ru

2 System Basics and Management

2.1 System Operation Basis

2.1.1 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.

2.1.2 System Operation Basic Functions

Table 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

2.1.2.1 Device Configuration Modes

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 five 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.

- Logging in to the device remotely through web. The device cannot be configured directly in this mode. That is, before configuration, some preparations need to be made.

2.1.2.2 Command Operating Modes

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 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. 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.

Mode	How to Enter the Mode	System Prompt	How to Exit the Mode	Functions
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.

2.1.2.3 Command Line Interface

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, run 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
   arl                Address translation item
   arp                Set a static ARP entry
   arp-security         To CPU arp security
   autosave           Auto save the startup configuration
   banner             Define a login banner
   bgp                BGP information
   cable-diagnostics     Cable Diagnostics on physical interface
.....  .....  .....
```

- 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-object           Show acl object
  arl                  Address translation item
  arp                  Command arp
  arp-security         To CPU arp security
  bfd                  BFD Protocol information
  bgp                  BGP information
  cable-diagnostics    Cable Diagnostics on physical interface
  card_list            Show information of hardware modules
  clock                Print system clock information
  cluster              Config cluster
  cpu                  Show CPU use per process
..... .....
```

- 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-object           Show acl object
  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 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

Error Message	Error Cause
	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 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	If a later history command is available, it is displayed. If no later command is available, the

To...	Press...	Execution Result
	keys	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 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

Key	Function
	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 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.

Key	Function
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.

2.2 System Login

2.2.1 Overview

The device supports the following system login modes:

- Logging into the device through the Console 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.
- WEB (remote login). Users can manage and maintain the device remotely in this mode.

2.2.2 System Login Function Configuration

Table 7 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	-

Configuration Tasks	
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.
Configuring remote login through web	Configure logging into the device via HTTP
	Configure logging into the device via HTTPS

Note

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

2.2.2.1 Log in to Device via Console Port

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 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.

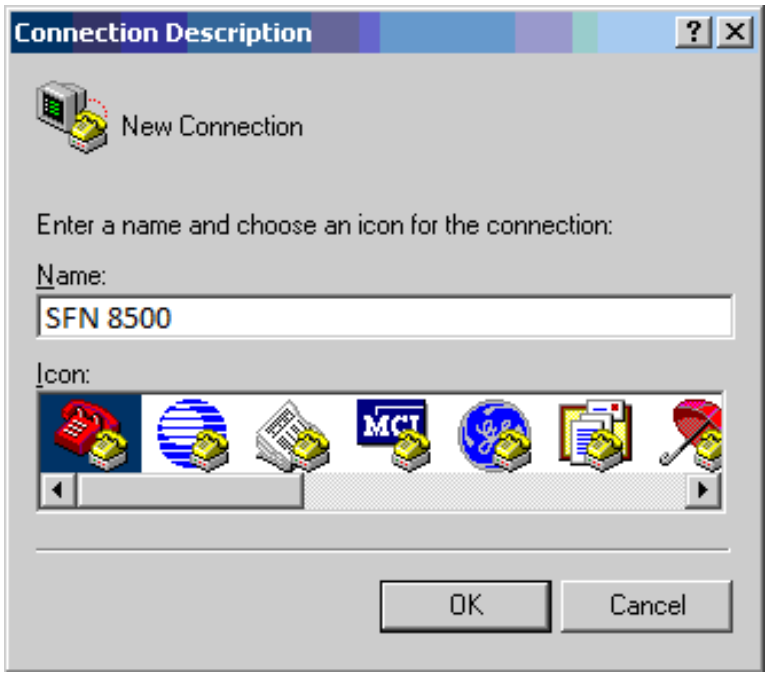


Figure 2 Creating a Connection

- Select a serial communication port:

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

Figure 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

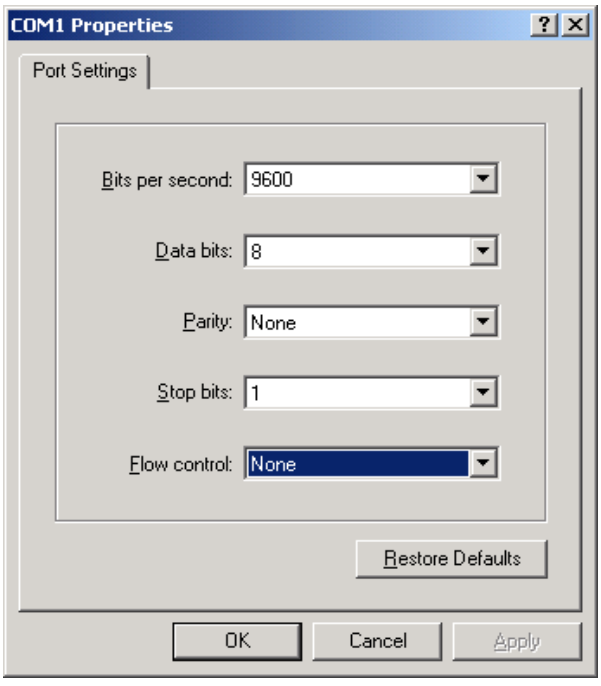


Figure 4 Configuring Parameters for the Serial Communication Port

- 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.

2.2.2.2 Configure Remote Login via Telnet

Configuration Condition

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 8 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 9 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.

2.2.2.3 Configure Remote Login via SSH

Configuration Condition

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 10 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** [*listen-port*][**sshv1-compatible**] [*listen-port*]	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 11 Taking an SSH Client for Remote Login

Step	Command	Description
Take the device as an SSH client for remote login.	**ssh** [**vrf** vrf-name] **version 1** remote-host port-number **[source-interface** interface-name **]** user [timeout] ssh [vrf *vrf-name*] version 2 *remote-host port-number* [source-interface *interface-name*] *user* [*timeout* | prefer-key { diffie-hellman-group-exchange-sha256 | diffie-hellman-group-exchange-sha1 | diffie-hellman-group14-sha1 | diffie-hellman-group1-sha1} | prefer-identity-key { ssh-rsa | ssh-dss } | prefer-ctos-cipher { aes128-cbc | 3des-cbc | blowfish-cbc | cast128-cbc | arcfour128 | arcfour256 | arcfour | aes192-cbc | aes256-cbc | rijndael-cbc-lysator.liu.se | sm4-cbc | aes128-ctr | aes192-ctr | aes256-ctr} | prefer-ctos-hmac { hmac-md5 | hmac-sha1 | umac-64-openssh.com | hmac-ripemd160 | hmac-ripemd160-openssh.com | hmac-sha1-96 | hmac-md5-96}]	Mandatory.

Note

- The SSH 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.

Take the Device as an SFTP Client to Access SFTP Server

The device acts as an SFTP client to log in to the specified SFTP server remotely through the SSHv2 protocol. During the login, a user name and a password are required for authentication from the SFTP server. After the SFTP client is connected to the SFTP server, download or upload the files on the server.

Table 12 Taking the Device as SFTP Client to Access the SFTP Server

Step	Command	Description
Take the device as the SFTP client to access the SFTP server.	sftp {get | put} [vrf vrf-name] remote-host port-number [source-interface interface-name] user password src-filename dst-filename [compress]	Mandatory

Note

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

2.2.2.4 Configure Remote Login via WEB

In order to facilitate the configuration and maintenance of network equipment, the device provides Web network management function. The device provides a built-in web server. You can log in to the device through a browser on PC, and configure and maintain the device intuitively by using the web interface. The device supports two

built-in web login modes: http login mode and HTTPS login mode. The device supports IPv4 web login and IPv6 web login.

Configuration Conditions

No

Configure Logging into Device via HTTP

Users can log into the device remotely through HTTP for related management and maintenance.

Table 13 Configure logging into the device via HTTP

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the HTTP server	ip http server	Mandatory By default, do not enable the web server.
Configure the port of the HTTP server	ip http port port_number	Optional By default, the port number of the HTTP server is 80.

Note

- Before starting the HTTP server, you must copy the corresponding WEB ROM file to /flash.

Configure Logging into Device via HTTPS

Users can remotely log into the device through the HTTPS mode for related management and maintenance, but before logging into the device through the HTTPS mode, they need to start the HTTPS service of the device.

Table 14 Configure logging into the device via HTTPS

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the HTTP server	**ip http server**	Mandatory By default, do not enable the WEB server.
Enable the HTTPS server	**ip http secure-server**	Mandatory By default, do not enable the WEB server.
Configure the port of the HTTPS server	**ip http port** *port_number*	Optional By default, the port number of the HTTPS server is 443.
Configure the certificate used by the HTTPS service	**ip http certificate** *ca-store*	Optional By default, the HTTPS service uses the self-signed certificate.

Note

- For the configuration of the trust domain and the import of the certificate, please refer to the relevant sections of PKI.

2.2.2.5 System Login Monitoring and Maintaining

Table 15 System Login Monitoring and Maintaining

Command	Description
show fingerprint	Display the fingerprint information of the SSH public key.
show ip http	Display the WEB configuration information

Command	Description
show ip http login-user	Display the information of the user that logs in via WEB successfully
show ip http restricted-user	Display the information of the user that fails to log in via WEB
show ip http statistics	Display the WEB server statistics information

2.2.3 Typical Configuration Example of System Login

2.2.3.1 Configure a Local Terminal to Telnet to the Device

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

Configuration Steps

Step 1: Create Virtual Local Area Networks (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.

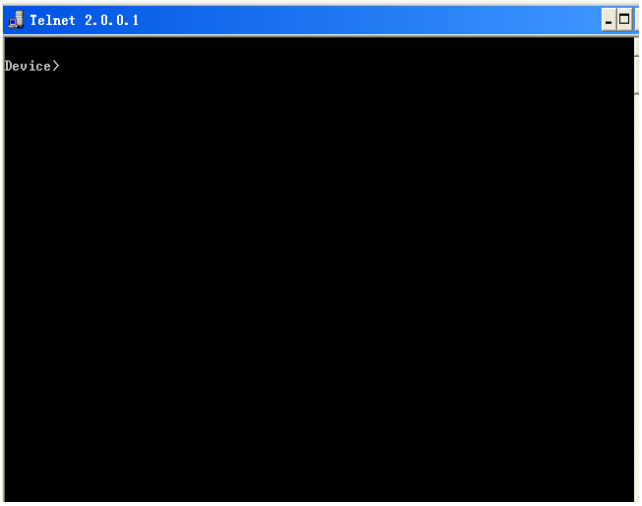


Figure 6 Window Displayed after Telnet Success

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.

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

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

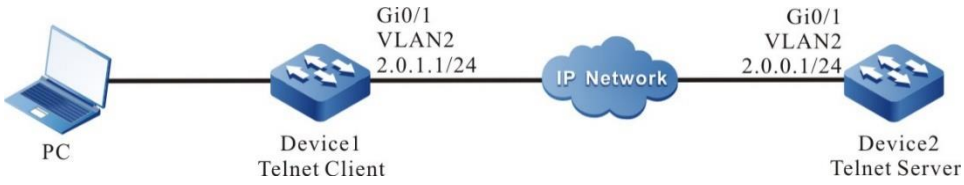


Figure 7 Network Topology for Configuring a Local Device to Telnet to a Remote Device

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 in line vty.

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

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

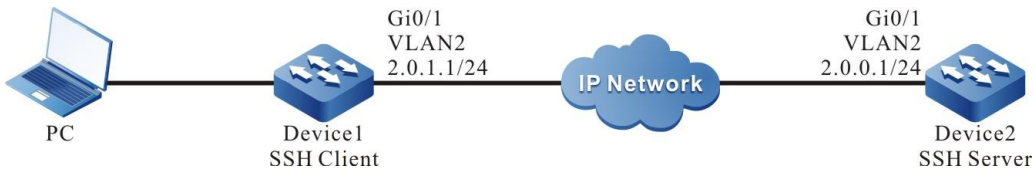


Figure 8 Network Topology for Configuring a Local Device to Log in to a Remote Device via SSH

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.

```
Device2#configure terminal
Device2(config)#local-user admin1 class manager
Device2(config-user-manager-admin1)#service-type ssh
Device2(config-user-manager-admin1)#password 0 admin1
Device2(config-user-manager-admin1)#exit
```

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 aaa
Device2(config-line)#exit
```

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

```
Device1#ssh version 2 2.0.0.1 22 admin1
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
admin1@2.0.0.1's password:
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.

2.2.3.4 Configure a Device as SFTP Client

Network Requirements

- PC acts as the SFTP server, Device acts as the SFTP client, and the network between the server and the device is connected.
- On the SFTP server, set the user name of the device logging into the FTP server to admin and the password to admin; place the files to be downloaded in the directory of the SFTP server.
- The device acts as the SFTP client to upload and download the file with the SFTP server.

Network Topology

Figure 9Network topology for configuring the device as the SFTP client

Configuration Steps

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

Step 2: Configure the SFTP server and place the files to be downloaded to the directory of the SFTP server (omitted).

Step 3: Configure the IP address of the device, making the network between the client and the server be connected (omitted).

Step 4: Device acts as the SFTP client to download and upload the file with the SFTP server.

Download one 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 in the Device 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.

#After copying, you can view whether the downloaded file exists in the Device file system and whether the uploaded file exists on the SFTP server (omitted).

```
Device(config-fs)#dir
 size        date      time      name
--------     ------    ------   --------
101526     MAR-01-2023  01:17:18   logging
10147      MAR-26-2023  07:58:50   startup
10207      MAR-01-2023  01:17:54   history
11676148   MAR-26-2023  07:51:32  sf8-g-6.6.7(46)-dbg.pck
2048       JAN-10-2023  17:30:20   snmp           <DIR>
```

2.2.3.5 Configure a Device as SFTP Server

Network Requirements

- Device acts as the SFTP server, PC acts as the SFTP client, and the network between the client and the server is connected.
- On the SFTP server Device, set the user name to admin1 and the password to admin1; the file system directory of Device acts as the root directory of the SFTP server.
- PC acts as the SFTP client to upload and download the file with the SFTP

server Device.

Network Topology

Figure 10 Network topology for configuring the device as the SFTP server

Configuration Steps

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

Step 2: Configure the IP address of the interface, making the network between PC and Device be connected (omitted).

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

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

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type ssh
Device(config-user-manager-admin1)#password 0 admin1
Device(config-user-manager-admin1)#exit
```

Enable the SSH service on Device (SFTP is one sub module of the SSH protocol.

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

Step 4 : Use PC as the SFTP client to upload and download one file to the SFTP server Device.

#The following takes the Linux system as an example to describe the related process.

#Input the correct IP address and user name, password to log into the SFTP server.

```
[root@aas ~]# sftp admin1@2.1.1.1
Connecting to 2.1.1.1...
admin@2.1.1.1's password:
sftp>
```

#Get the startup file in the file system of the SFTP server Device.

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

#After copying the file, you can find the related file in the operated 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 the file in PC to the file system of the SFTP server Device.

```
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
```

#After uploading the file, you can find the corresponding file in the file system of Device.

```
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
```

2.2.3.6 Configure a Local Device to Log in to a Remote Device via SSH Public Key Authentication Mode

Network Requirements

- PC acts as the local terminal and installs the SecureCRT software.
- PC acts as the local terminal and can access Device via the SSH public key.

Network Topology

Figure 11Network topology of configuring a local device to log in to a remote device by the SSH public key authentication mode

Configuration Steps

Step 1: Configure the IP address of the interface and configure the routing protocol to make the PC and Device intercommunicate with each other (omitted).

Step 2: Configure the SSH service and FTP function.

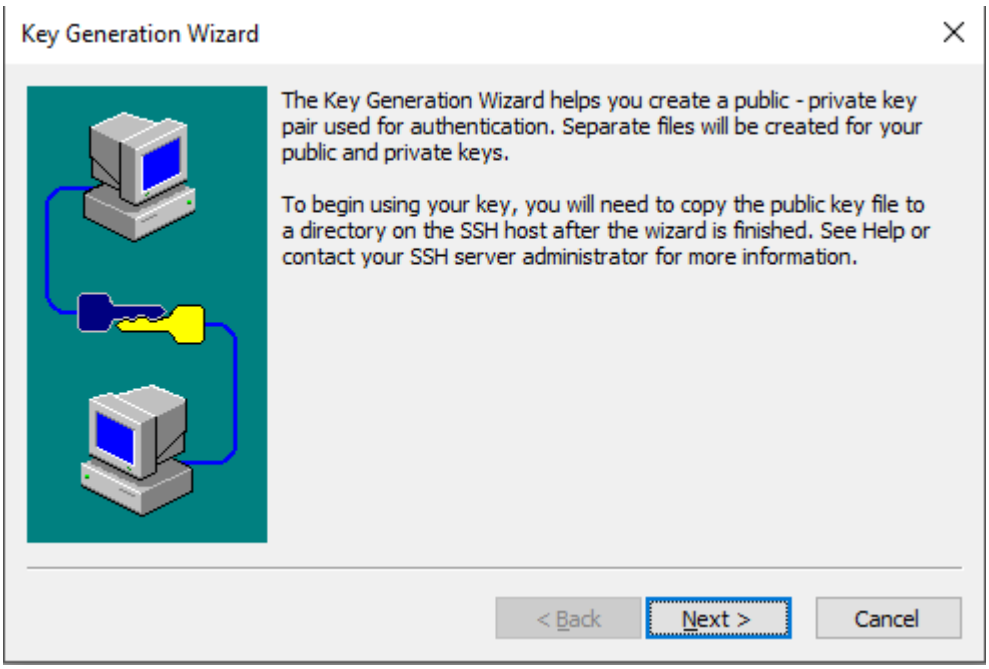
```
Device#configure terminal
Device(config)#ip ssh server
```

Step 3 : Configure the login user name of Device.

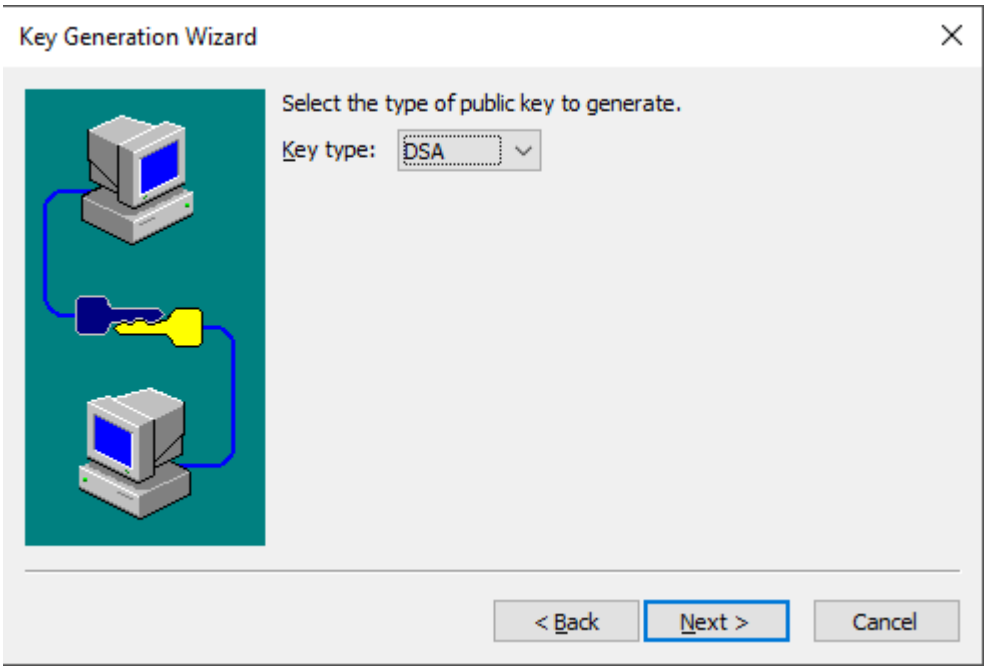
```
Device(config)#local-user user1 class manager
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#exit
```

Step 4 : On PC, generate the SSH public key file.

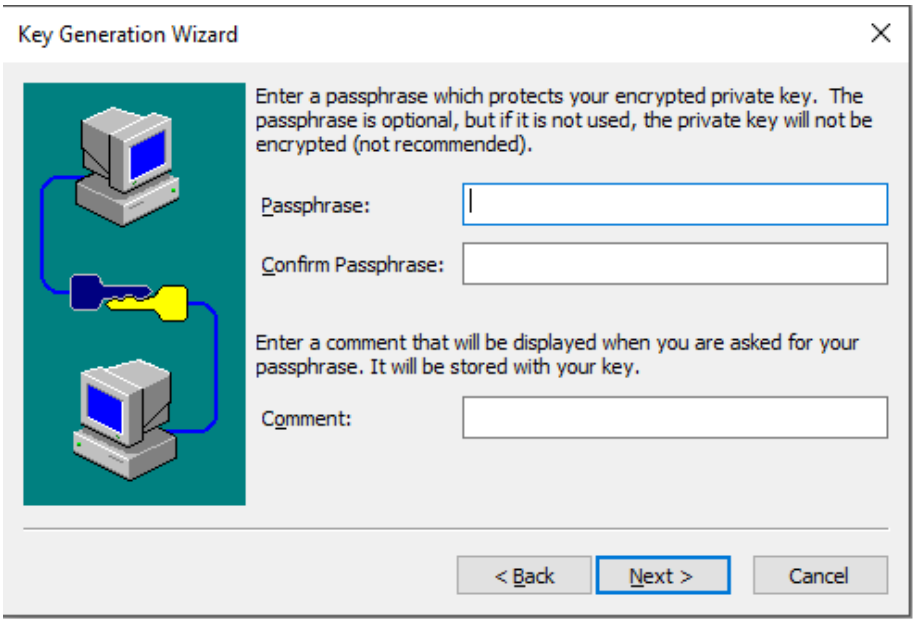
#The document takes Windows operation system as an example. SecureCRT uses Version 6.1.2. On PC, open the SecureCRT software tool bar and click the **Tools** button. In the drop-down menu, click **Create Public Key (C)** to display the wizard of generating the key, and click **Next**.



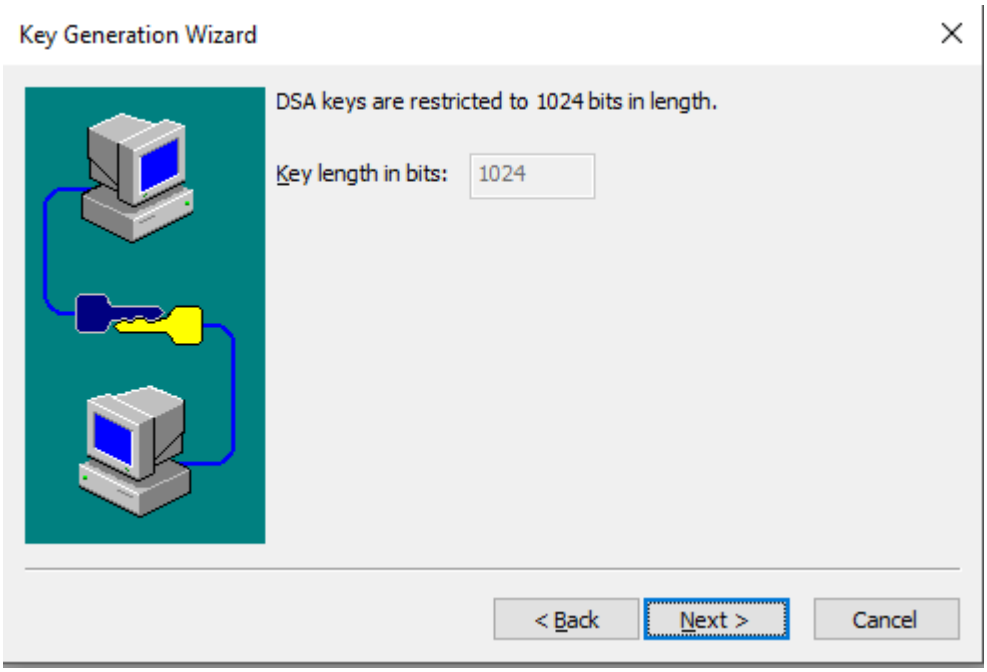
#Key type: Select any one from DSA and RSA. Here, take DSA as an example and click **Next**.



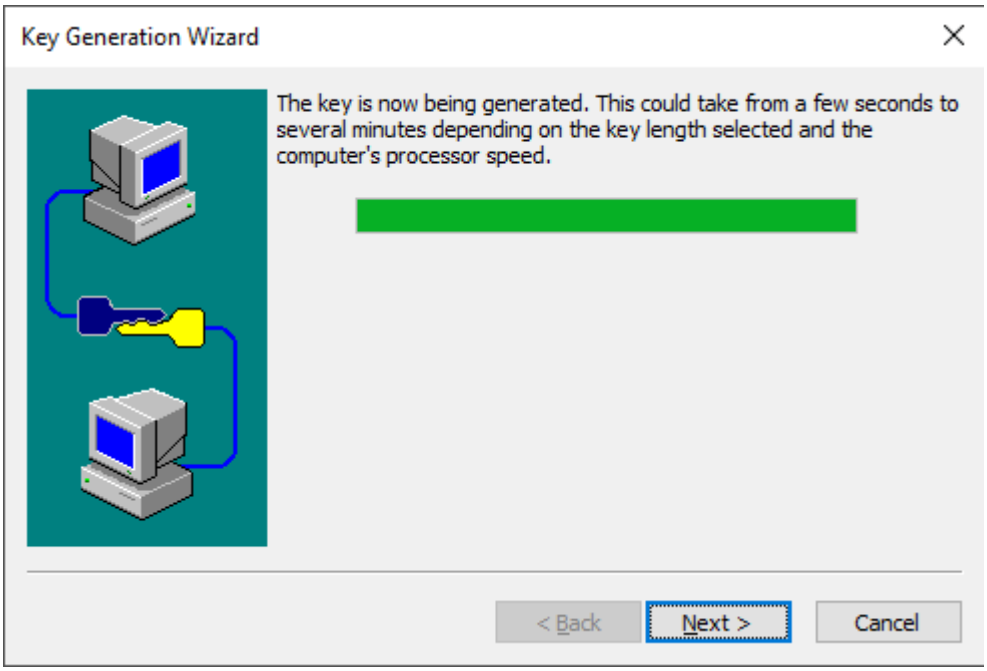
#The pass phrase is taking effect at the local and you can ignore. Click **Next**.



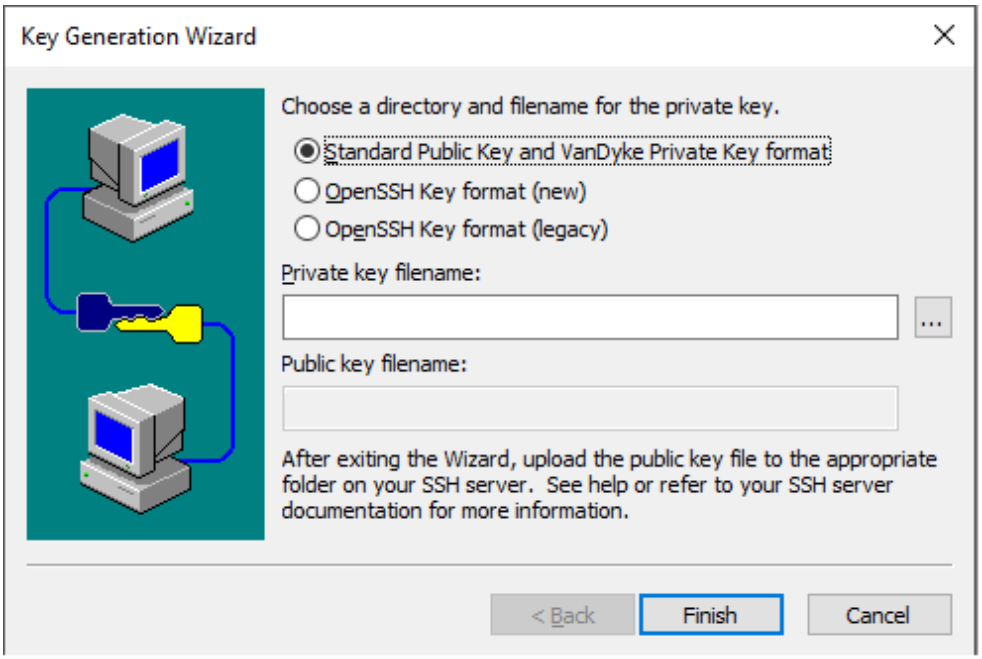
#Fill in the key length according to the description and click **Next**.



#To generate the key, you need to move the mouse continuously. After generating the key, click **Next**.



#Select the format of storing the key. Here, select the **OpenSSH key format** and click **Finish**.



#In the FTP server path of the PC, create the file “authorized_keys”, copy all content of the public key file “Identity.pub” to “authorized_keys”, and copy the file “authorized_keys” to /flash/sshpubkey/user1/.

```
Device#filesystem
Device(config-fs)#mkdir sshpubkey
Device(config-fs)#cd sshpubkey
Device(config-fs)#mkdir user1
Device(config-fs)#cd user1
Device(config-fs)#copy ftp 2.0.0.1 username password authorized_keys file-system authorized_keys
```

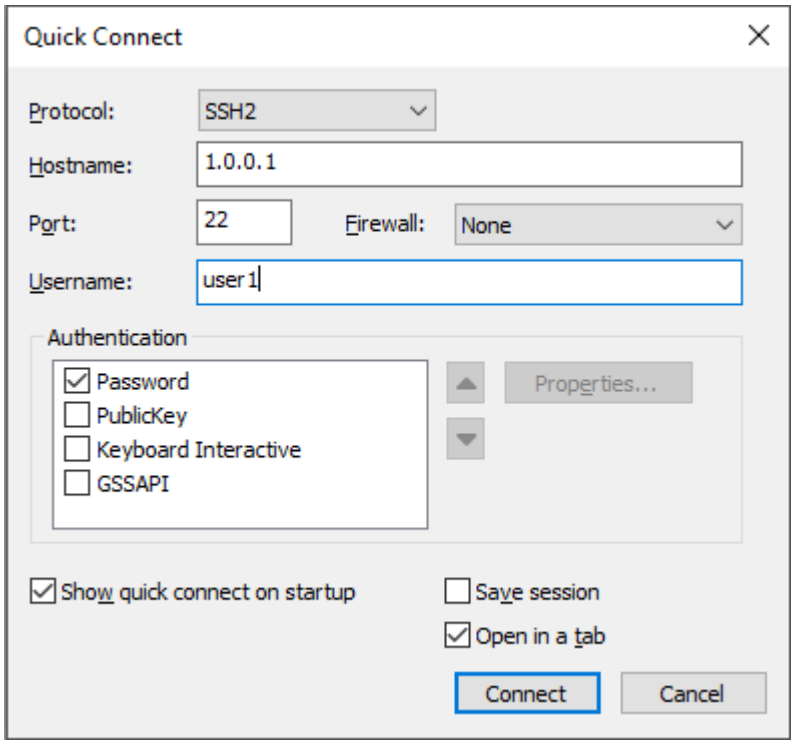
Note

- For the format of storing the key, select OpenSSH and the other formats are not supported.
- When copying the “Identity.pub” content, select all and then copy, and do not need to change a line.
- When multiple clients use one user to log in, change a line after the public key information stored by “authorized_keys”, then paste the information of another public key, and superimpose.

- By default, the device does not have the directory /flash/sshpubkey/user1/, and you need to create in filesystem. User1 in the directory is the user name used by authentication. The user name is the user on the device. If the user name is user2, create /flash/sshpubkey/user2/.
- SSH public key authentication does not support SSHv1.

Step 5: Check the result.

PC uses the SecureCRT software to set up the SSH connection, use publickey first or unique authentication, click **Connect**, and you can see that the connection is not required to input the password, but can log into the device directly.



2.2.3.7 Configure the Local Device to Log into a Remote Device via WEB

Network Requirements

- Use PC as local terminal to log into the device through web.
- The route between the two devices must be reachable.

Network Topology

Figure 12 Configure the local device to log into the remote device via web

Configuration Steps

Step 1: Configure the local user and the related attributes.

```
Device>enable
Device#configure terminal
Device(config)#local-user admin class manger
Device(config-user-manager-admin)password 0 admin
Device(config-user-manager-admin)service-type web
```

Step 2: Enable the https service.

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

Step 3: Check the result.

Open the browser on the PC and enter http://2.0.0.1 in the browser address bar, after successful web login, you will enter the web interface of the device.

2.3 System Control and Management

2.3.1 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.

2.3.2 Login Control and Management Function Configuration

Table 16 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.
	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.

Configuration Tasks	
	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.

2.3.2.1 Switch Over Between User Levels

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 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-method none** is configured, no password is required.

b) If **aaa authentication enable-method enable** is configured, and the enable password is configured, use the password for authentication. Otherwise, the "% Bad passwords " 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 Condition

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 17 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.

2.3.2.2 Configure the Command Level

Configuration Condition

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 18 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.

2.3.2.3 Configure the enable Password

Configuration Condition

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 19 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.

2.3.2.4 Configure Line Properties

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 Condition

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 20 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 21 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 22 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 23 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 Access Control List

Set the access control list of the user. Only the hosts permitted by the access control list can log into the device.

Table 24 Configure the line access control list

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the line configuration mode of the Console port or VTY.	line { vty vty-min-number [vty-max-number] }	Mandatory
Configure the access control list	access-class { access-list-number | access-list-name} { in | out}	Mandatory
Configure ipv6 ACL control list	ipv6 access-class{access-list-number | access-list-name }{ in | out}	Optional

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 25 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 26 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 27 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 28 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 password authentication mode: Uses line password authentication.
- Login aaa authentication mode: Uses the AAA authentication.
- No login indicates that no authentication is required for login.
- By default, the no login authentication mode is used for Telnet, and the local user authentication mode is used for SSH.

Table 29 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 {aaa [*domain-name* | default] | password}	The command will affect the AAA authentication, authorization, and accounting.

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 30 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.

2.3.2.5 System Control and Management Monitoring and Maintaining

Table 31 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.

2.4 FTP, FTPS, TFTP and SFTP

2.4.1 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.

FTPS is one enhanced FTP protocol of using the standard FTP protocol and commands, adding the SSL security function for the FTP protocol and data channel. FTPS is also called FTP-SSL and FTP-over-SSL. SSL is one protocol of encrypting and decrypting the data in the security connection between the client and the server with the SSL function. On the device, only the FTP client supports the function.

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.

SFTP (Secure File Transfer Protocol /Secure FTP) is the new function in SSH 2.0. SFTP is based on the SSH connection so that the remote user can log into the device safely for managing the file, transmitting the file and other operations, providing higher security guarantee for the data transmission. SFTP provides one safe method for transmitting the file. SFTP is the sun function of SSH, realizing the safe transmission of the file. SFTP encrypts the transmitted authentication information and transmitted data, so using SFTP is safe. If the requirement for the network security is higher, you can use SFTP to replace FTP, but the SFTP file transmission adopts the encryption/decryption technology, so the transmission efficiency is lower than the FTP file transmission.

2.4.2 FTP, FTPS, TFTP and SFTP Function Configuration

Table 32 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.
Configure a TFTP client.	Configure the functions of a TFTP client.
Configure an SFTP server	Configure the functions of the SFTP server
Configure an SFTP client	Configure the functions of the SFTP client

2.4.2.1 Configure an FTP Server

Configuration Condition

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 33 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

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

2.4.2.2 Configure an FTP Client

Configuration Condition

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 34 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.
Configure the FTP client to use the port mode first	ip ftp port-first	Optional. By default, first use the passive mode and the server to set up the data connection.

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.

2.4.2.3 Configure FTPS Client

Configuration Condition

None

Configure FTPS Client Function

When copying files on the device with the **copy** command (see the relevant chapter of "File System Management"), the device can be triggered to establish a connection with the remote FTPS server as an FTPS client.

Table 35 Configure the FTPS client function

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Configure the PKI trust domain name of the FTPS client	**ip ftp secure-identity** *ca-name*	Mandatory By default, do not configure the PKI trust domain name of the FTPS client.

2.4.2.4 Configure a TFTP Client

Configuration Condition

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 36 Configuring the Functions of a TFTP Client

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the source address of the	ip tftp { source-interface *interface-name*	

Step	Command	Description
TFTP client.	| source-address *ip-address* }	

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.

2.4.2.5 Configure a TFTP Server

Configuration Condition

None

Configure the Functions of a TFTP Server

To configure a device as the TFTP server, first enable the TFTP server function so that the TFTP client can access.

Table 37 Configuring the Functions of a TFTP Server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the functions of the TFTP server	tftp enable	Mandatory By default, do not enable the functions of the TFTP server.

2.4.2.6 Configure an SFTP Server

Configuration Condition

None

Configure the Functions of an SFTP Server

Before configuring the device as the SFTP server, first enable the SFTP server function. Then, the SFTP client can access the SFTP server. Because SFTP is one subsidiary function of SSH, to enable the SFTP server function of the device, you also need to enable the SSH server function of the device.

Table 38 Configuring the SFTP server function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the IPv4 SSH server function	ip ssh server [sshv1-compatible] [*listen-port*]	Mandatory By default, do not enable the IPv4 SSH server function.
Enable the SFTP server function	sftp server enable	Mandatory By default, do not enable the SFTP server function.

Table 39 Configure IPv6 SFTP server function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the IPv6 SSH server function	ipv6 ssh server [sshv1-compatible] [listen-port]	Mandatory By default, do not enable the IPv6 SSH server function.
Enable the SFTP server function	sftp server enable	Mandatory By default, do not enable the SFTP server function.

2.4.2.7 Configure a SFTP Client

Configuration Condition

None

Configure the Functions of an SFTP Client

The device serves as the SFTP client and connects the SFTP server, downloading the file from the SFTP server or uploading the file to the SFTP server.

Table 40 Configuring the function of an SFTP client

Step	Command	Description
Configure the device as the SFTP client to upload or download the file to 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

2.4.2.8 FTP and TFTP Monitoring and Maintaining

None

2.4.3 Typical Configuration Example of FTP and TFTP

2.4.3.1 Configure a Device as an FTP Client

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 13 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.

#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.

2.4.3.2 Configure a Device as an FTP Server

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 admin1, and the password is admin1. 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

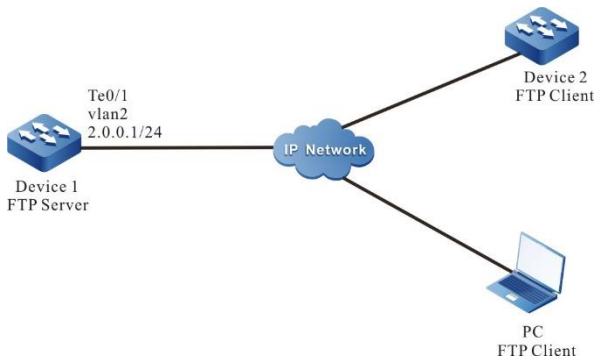


Figure 14 Networking in Which a Device Acts as an FTP Server

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)#local-user admin1 class manager
Device1(config-user-manager-admin1)#service-type ftp
Device1(config-user-manager-admin1)#password 0 admin1
Device1(config-user-manager-admin1)#exit
```

#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          (state)
-------- ----- ------ ------  -------------------- --------------------  -------
27cf8a4  TCP       0      0  0.0.0.0.80          0.0.0.0               LISTEN
27ce0a4  TCP       0      0  130.255.104.43.22    130.255.98.2.3590       ESTABLISHED
27d0be4  TCP       0      0  0.0.0.0.21          0.0.0.0               LISTEN
27d0824  TCP       0      0  127.0.0.1.2622       127.0.0.1.1026          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 admin1 admin1 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>
```

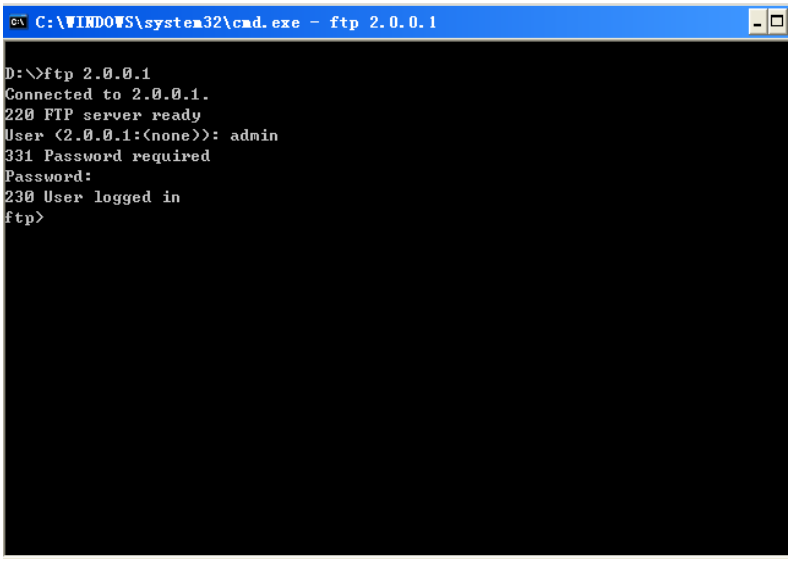


Figure 15 Logging in to the FTP Server via the Windows DOS Screen

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

```
ftp>binary
```

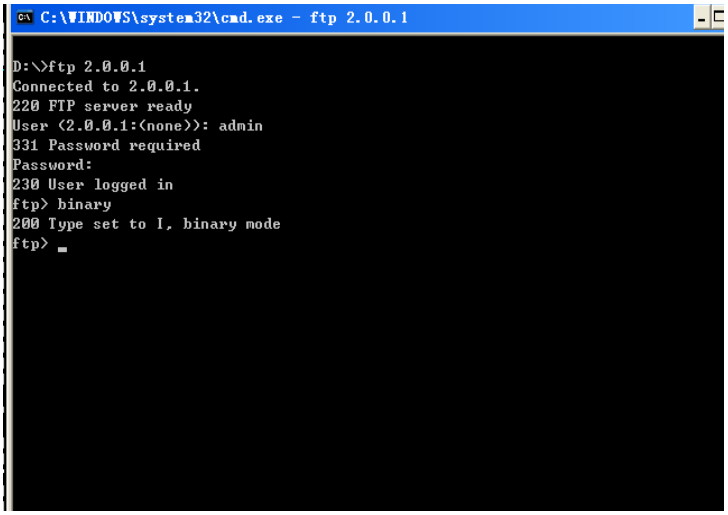


Figure 16 Configuring the PC and FTP Server to Transmit data in Binary Mode

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

```
ftp>get startup
```

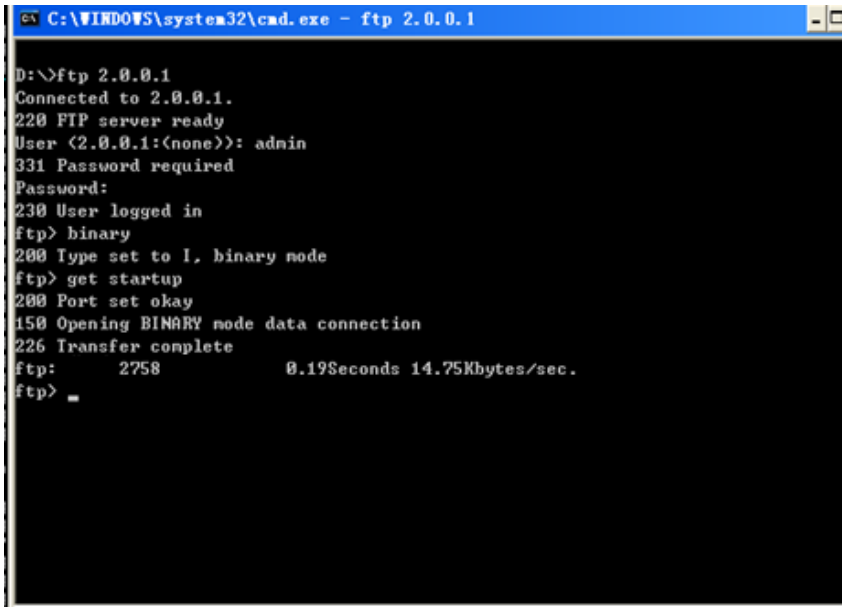


Figure 17 Copying a Configuration File from the FTP Server

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.
- As the FTP server, the device is restricted to strict mode. By default, only supporting the passive mode to transmit files. It needs to use **security-mode loose** to modify the mode to loose mode to support the active mode for

transmitting files.

2.4.3.3 Configure a Device as an TFTP Client

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 18 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.

2.4.3.4 Configure a Device as an SFTP Client

Network Requirements

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

Network Topology

Figure 19 Networking for configuring a device as an SFTP client

Configuration Steps

Step 1: Configure an SFTP server, and place the files to be downloaded in the SFTP server directory. (Omitted)

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

Step 3: Device acts as the SFTP client to upload files to and download files from the SFTP server.

#Download one 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 of the Device 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 4: Check the result.

#After copying, you can view whether the downloaded file exists in Device file system; view whether the uploaded file exists on the SFTP server (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>
```

2.4.3.5 Configure a Device as an SFTP Server

Network Requirements

- A PC acts as an SFTP server, and Device acts as an SFTP client. The network between the server and the device is normal.
- On the SFTP server, the user name for a device to log in to the SFTP server is admin1, and the password is admin1. The file system directory of Device serves as the root directory of the SFTP server.
- The PC acts as the SFTP client to upload files to and download files from the SFTP server.

Network Topology

Figure 20 Networking for configuring a device as an SFTP server

Configuration Steps

Step 1: Configure the IP address of the interface so that the network between the PC and the Device is normal. (Omitted)

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

On the SFTP server Device, configure the authorized user name and password.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type ssh
Device(config-user-manager-admin1)#password 0 admin1
Device(config-user-manager-admin1)#exit
```

#On the Device, enable the SSH service (SFTP is one sub module of the SSH protocol).

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

Step 3: Use the PC as the SFTP client to upload and download one file to the SFTP server Device.

#The following takes the Linux system as an example to describe the related process.

#Input the correct IP address and user name, password to log into the SFTP server.

```
[root@aas ~]# sftp admin1@2.1.1.1
Connecting to 2.1.1.1...
Admin1@2.1.1.1's password:
sftp>
```

#Get the startup file in the file system of the SFTP server Device.

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

#After copying the file, you can find the related file in the operation 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 the file in the PC to the file system of the SFTP server Device.

```
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
```

#After uploading the file, you can find the corresponding file in the file system of Device.

```
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
```

2.4.3.6 Configure a Device as an FTPS Client

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the Device and the Client is normal.
- Set up the security data channel between FTP Server and FTP Client, providing the security guarantee for the data transmission.
- The file can be uploaded and downloaded between FTP Client and FTP Server.

Network Topology

Figure 21 Networking for configuring a device as an FTPS client

Configuration Steps

Step 1: Configure the IPv4 address of the interface (omitted).

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

Step 3: FTP Client imports the FTP CA certificate, user certificate, and private key.

#Create one domain test on the device:

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

#Bind FTP with the domain test:

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

#Open the CA certificate (rsaRoot.cer) by the notepad, copy the content, input **crypto ca import certificate to test** on the shell, and import the certificate to the device domain test according to the prompt:

```
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
A4GMADCBiAKBgHXZMtpxzH8p0uUt6QomUhuJNcy9iyYhoJVx4l3T6kpmx9cdzapM
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) and the private key certificate (topsec_rsa2_myself.key) by the notepad, copy the content, input the command **crypto ca import certificate to test** on the shell, and import the certificates to the device domain test according to the prompt in turn:

```
Device(config)#crypto ca import certificate to test
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDVTCCAr6gAwIBAgIQEJ7twbl3pDlzJz99DFOKOzANBgkqhkiG9w0BAQUFADBiMQswCQYD
VQQGEwJDTjEQMA4GA1UECAwHQkVJSklORzEOMAwGA1UECgwFQ0lFQ0MxDzANBgNVBAs
MBkdGQSBDQTEgMB4GA1UEAwwXTWluaUNBIEZyZUJTRCBSb290IENlcnQwHhcNMTIwNjI2M
DUwMTIzWhcNMzIwNjI2MDUwMTIzWjB/MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHYmVpa
mluZzESMBAGA1UEBwwJZG9uZ2NoZW5nMQ4wDAYDVQQKDAVjaWVjYzEMMAoGA1UECwwD
Z2ZhMR0wGwYJKoZIhvcNAQkBFg50ZXN0QGVjLmNvbS5jbjENMAsGA1UEAwwEcnNhMjCBnz
ANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA6AlNqTnNsV9Yyij2tTMppB9C5VCLtkPh9Kllq/ZTl
```

VhrJED+N5HVfQQyZYS/z4JWAip50dyP1+NP+bvP+pb9CfEaJ8+ObYQnfUH6qiPccLkWO3XYanu
6Dw5EMJYntwglSKmk1Pcc+j+yzWnwYMDFcbSsQ+8J5UzlesFhU7GnXacCAwEAAaOB7jCB6zA
+BgNVHR8ENzA1MDOgMaAvhi1odHRwczovLzIxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwvU
lNBMTAyNC5jcmwwUQYDVR0gBEowSDBGBggrBgEEAYcrMjA6MDgGCCsGAQUFBwIBFixodH
RwczovLzIxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwvUlNBMTAyNC5wbDALBgNVHQ8EBA
MCA/gwCQYDVR0TBAIwADAdBgNVHQ4EFgQUp/9/ODGLR84syxPaBkLG3mCpU5YwHwYDVR
0jBBgwFoAUhnY8uZXbE2iX1mXOipvfuDUgAeswDQYJKoZIhvcNAQEFBQADgYEAYrFZQrINHoL
N9odcGctzTRGVmMcv9sJ0ncgUEfbrLu6QUodQy3jjxWFIxheJK1btfF66/ShuKtZpqJ1WE9l92tfIH
wLpXT0gujtxNi02TOPBNEU7P9nUgxgfDG+uhyPTeufSkfn3LCTHmGfVORF2soGSlaUPV1Zy5E9h
mFZoMhs=-----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-----

MIICXQIBAAKBgQDoCU2pOc2xX1jKKPa1MymkH0LlUlu2Q+H0qUir9lOVWGskQP43kdV9BDJlhL
/PglYCKnnR3I/X40/5u8/6lv0J8Ronz45thCd9QfqqI9xwuRY7ddhqe7oPDkQwlie3CCVIqaTU9xz6
P7LNafBgwMVxtKxD7wnlTOV6wWFTsaddpwIDAQABAoGBAMnJNWliJFgI4+1CvHGN4buhmAp
WBnnmBL1A7jrlh4CMGPi5MJrgzvjeSnlwfWIXJXbSu4feuJT1UFqMkuyIm9l+k8Rm3hjClXIlfNV/
ykG6a6GIVFYGxQWhaL50Pm6S7xXL9Ryd6hnOHUUtwuLvkpBTx/4qvrIABDtXRjVglvApAkEA9B
N1ZxM31BOyeB6KXvvmXD6/+dGaDfE4Dbcijy1LgKliaEBJ00e/0R9ekg6myGTU2asJvPtkaXPqcw
vU6+e2mwJBAPNfRTk9LzUlNmTV2DrsE9k3rbPnqqS9wb/mLUNdv2FQeoY/Zf4qh0WXsug2q/6
GPsvLUA7mbdArGFUwwQbw3+UCQQC8r25LSOgX40JM6g8+bq4fEcOHdSoLLTeQIststC9yP3/
75/cqhoUbPYz2jK0SriB+RWM53X46p4nPdo4b8P2RAkBGjoBLL+nXxooWgcjGjFrUxsedOLTIPh
tFvz2wliWx2NsswISZQ0skae58VB1ZFSJvguoa58M+bsAHMrNDh+HhAkBcNAjKBDdVw0ll6bN
oRGugEvuo3Z3O0kbVcjzZld+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.

#After importing the certificate successfully, you can use the command **show crypto ca certificates** to view that the status is Valid.

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: Upload and download the file between FTP Client and FTP Server.

#FTP Client uploads the file to the FTP Server.

```
Device#filesystem
Device1(config-fs)#copy file-system startup ftps 1.0.0.1 a a startup VerifyType peer

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

#FTP Client downloads the file from FTP Server.

```
Device(config-fs)#ftpscopy 1.0.0.1 a a test.doc test.doc VerifyType peer

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

Step 5: Check the result.

#After downloading, view the downloaded file in the file system of Device.

```
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
```

2.5 File System Management

2.5.1 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.
- USB: Used to save the user data.
- 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.

Note

- The filesystem command is used to enter the file system, and can be used on both the master control and standby control.

2.5.2 File System Management Function Configuration

Table 41 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.

2.5.2.1 Manage Storage Devices

Configuration Condition

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 42 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 the Storage Devices

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

to format the storage device.

Table 43 Formatting a Storage Device

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

Caution

- 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.

2.5.2.2 Manage File Directories

Configuration Condition

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 44 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 45 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 46 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 47 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 48 Deleting a Directory

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

2.5.2.3 Manage File Operations

Configuration Condition

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 49 Copying a File

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

Rename a File

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

Table 50 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 51 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 52 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.

2.5.2.4 Download a File from FTP

Configuration Condition

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 53Download 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 | /syslog | /usb | *dest-filename* } ftpscopy [vrf *vrf-name*] *host-ip-address usrname password src-filename* { /flash | /syslog | /usb | dest-filename } VerifyType { none | peer }	Optional

Note

- The **ftpcopy** and **ftpscopy** 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** and **ftpscopy** command in the technical manual.

2.5.2.5 Configure Startup Parameters

Configuration Condition

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 54 Configuring Startup Parameters

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

2.5.2.6 File System Managing, Monitoring, and Maintaining

Table 55 File System Managing, Monitoring, and Maintaining

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	Display the storage location information of the system file in the file system
show file descriptor	Display the file descriptor information of the system file in the file system
show boot-loader	Display the system startup parameters.

2.5.3 Typical Configuration Example of File System Management

2.5.3.1 Configure Startup Parameters

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/sp26-g-9.5.0.2(20)(R).pck
The app to boot at the this time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
Boot-loader0: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck

Device(config-fs)#exit
```

#Modify the file for next startup to the sp26-g-9.5.0.2(20)(R).pck file that is stored in the flash, and set the priority to 0.

```
Device#filesystem
Device(config-fs)#boot-loader /flash/sp26-g-9.5.0.2(20)(R).pck

Boot-loader0 set OK
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/sp26-g-9.5.0.2(20)(R).pck
```

```
The app to boot at the this time is: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck

Boot-loader0: flash0: /flash/sp26-g-9.5.0.2(20)(R).pck
Boot-loader4: backup0: sp26-g-9.5.0.2(20)(R).pck
Device(config-fs)#exit
```

2.6 Configuration File Management

2.6.1 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.

2.6.2 Configuration File Management Function Configuration

Table 56 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.
Encrypt the configuration file	Encrypt the boot configuration
Auto save configuration	Auto save configuration

2.6.2.1 Save the Current Configuration

Configuration Condition

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 57 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.

2.6.2.2 Configure the Backup System

Configuration Condition

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 58 Backing Up the Current Configuration

Step	Command	Description
Enter the file system configuration mode.	filesystem	-
Back up the current configuration to a	copy running-config { file-system *dest-*	Mandatory

Step	Command	Description
remote host through the FTP protocol.	*filename* | ftp [vrf *vrf-name*] { *hostname* | *ip-address* } *username password dest-filename* | startup-config | tftp [vrf *vrf-name*] { *hostname* | *ip-address* } *dest-filename* ftps [vrf *vrf-name*] { *hostname* | *ip-address* } *username password dest-filename* VerifyType { none | peer } }	

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 59 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 | ftps [vrf vrf-name] { hostname | ip-address } username password dest-filename VerifyType { none | peer }| tftp [vrf vrf-name] { hostname | ip-address } dest-filename }	Mandatory

2.6.2.3 Restore the Startup Configuration

Configuration Condition

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 60 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* | ftps [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.

2.6.2.4 Configuration File Encryption

Configuration Condition

- To encrypt the configuration file, you need to insert the USB device.

Configure Configuration File Encryption

The configuration file encryption adopts the SM4 algorithm to encrypt the configuration file. The key is specified by the user. After the user specifies the key, encrypt the configuration file when executing the write action next time.

Operation record encryption adopts the SM4 algorithm to encrypt the configuration and the key is specified by the user. After the user specifies the key, start encrypting the subsequent operation record.

Table 61 Configuration file encryption and operation record encryption

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

Note

- The configuration file encryption takes effect during the next write action after configuring the encryption function. The operation record encryption takes effect at once after configuring the encryption function.
- To configure the encryption function, you need to insert the external USB device. The operation record encryption function does not need the USB

device.

2.6.2.5 Auto Save Configuration

Configuration Condition

None

Auto Save Configuration

Auto saving refers to automatically saving the operation configuration of the device after the device is opened according to the configuration rules.

Table 62 Auto save configuration

Step	Command	Description
Enter the global configuration mode	config terminal	-
Enable auto saving	configuration-file auto-save enable	Enable the function of auto saving the configuration
Configure the interval of auto saving	configuration-file auto-save interval *interval*	The interval for automatically saving the configuration. The value range is 30-43200, in minutes. The default value is 30.
Configure auto saving CPU utilization threshold	configuration-file auto-save cpu-limit *cpu-usage*	Automatically save the configured CPU utilization threshold. The value range is 1 -100, and the default value is 50.
Configure auto saving delay time	configuration-file auto-save delay *delay-interval*	The delay time for automatically saving the configuration after the configuration changes. The value range is 1-60, in minutes. The default value is 5.

Note

When the following conditions occur, the system will cancel the operation of automatically saving the configuration file:

- There is currently an operation of writing configuration file.
- The device is in the process of configuration recovery.
- The CPU utilization is high.

2.6.2.6 Configuration File Managing, Monitoring, and Maintaining

Table 63 Configuration File Managing, Monitoring, and Maintaining

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

2.7 System Management

2.7.1 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

2.7.2 System Management Function Configuration

Table 64 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.
Configure the encryption service.	Configure the encryption service.
Configure the history command saving	Configure the history command saving function.

Configuration Tasks	
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.

2.7.2.1 Configure the Device Name

Configuration Condition

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 65 Configuring the Device Name

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

2.7.2.2 Configure the System Time and Time Zone

Configuration Condition

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 66 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

2.7.2.3 Configure the Login Welcome Message

Configuration Condition

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 67 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

2.7.2.4 Configure the System Exception Processing Mode

Configuration Condition

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 three 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. Besides, you can configure the processing mode of the health detection exception, and the processing modes include ignore and restart.

Table 68 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 }] | detect-health {ignore | reload} }	Mandatory. By default, periodical exception detection is enabled, and the exception level set for device restart is critical. By default, the health detection is enabled. After the device health detection becomes abnormal, the processing mode is ignore by default.
Configure the mode of processing the abnormality in the VST mode	exception { period-detect enable | reboot {device *device-num* | level device *device-num* { alert | critical | emergency | error | warn } } | detect-health *device-num* {ignore | reload} }	Mandatory. By default, the periodical abnormal detection is enabled. When the abnormality appears, the abnormal level of the device

Step	Command	Description
		restarting is critical. By default, the health detection is enabled. After the device health detection becomes abnormal, the processing mode is ignore by default.

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.

2.7.2.5 Configure to Restart a Device

Configuration Condition

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 69 Restarting a Device

Step	Command	Description
Use a command to restart the device or in the VST mode, use the	reload	Mandatory

Step	Command	Description
command to restart all in-place virtual switch devices in the VST domain		

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.

2.7.2.6 Configure the History Command Saving Function

Configuration Condition

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 70 Configuring the History Command Saving Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure to save history commands.	shell-history save	Mandatory. By default, the history command

Step	Command	Description
		saving function is enabled.

2.7.2.7 Configure the Login Security Service

Configuration Condition

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 or the login request from the user 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 71 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 { telnet | ssh | ftp | snmp}	Mandatory. By default, the system login

Step	Command	Description
		security service is enabled.

Configure the Parameters of the System Login Security Service

Table 72 Configuring the Parameters of the System Login Security Service

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the login time of the IP address forbidden by the Telnet module	login-secure telnet ip-addr forbid-time *forbid-time-number*	Mandatory By default, it is 10 minutes.
Configure the maximum successive login authentication failure times of the IP address forbidden by the Telnet module	login-secure telnet ip-addr max-try-time *max-try-time-number*	Mandatory By default, it is 5 times.
Configure the age time of the information recorded by the IP address forbidden by the Telnet module	login-secure telnet ip-addr record-aging-time *record-aging-time-number*	Mandatory By default, it is 15 minutes.

2.7.2.8 Configure CPU Monitoring

Configuration Condition

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 73 Configuring CPU Monitoring

Step	Command	Description
Enter the privileged mode	enable	-
Enable CPU occupancy monitoring of the processes.	spy cpu	Mandatory. 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.

2.7.2.9 Configure Display of Properties in Pages

Configuration Condition

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 74 Configuring Display of Properties in Pages

Step	Command	Description
Enter the privileged mode.	enable	-
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.

2.7.2.10 Operation Record File Management

Configuration Condition

None

Configure Operation Record File

The operation record is saved in the flash by default. The operation record file management is mainly to change the saving location of the operation record.

Table 14 Configuration file encryption, operation record encryption

Step	Command	Description
Enter the global configuration mode.	**config terminal**	-
Operation record file management	**shell-history location** *device-name*	The user specifies the saving location of the operation record.
Specify the size of the operation record file	**shell-history file max-size** *num*	The user specifies the size of the operation record file.

2.7.2.11 System Management Monitoring and Maintaining

Table 75 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 device	Display the device information of the system.
show environment	Display the information about the board temperature.
show history | { begin *expression* | exclude *expression* | include *expression* | redirect { file *file-name* | ftp [vrf *vrf-name*] { *hostname* | *ip-address* } *user-name password file-name* | ftps [vrf *vrf-name*] { *hostname* | *ip-address* } *user-*	Display the information about history commands.

Command	Description
name password file-name } }	
show language	Display the information about system language version.
show login-secure { telnet | ssh | ftp | snmp}{ip-addr | user | quick-connect}	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	Display the 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 [brief]	Display the fan information.
show system lpu [*lpu-num* | brief]	Display the LPU information
show system module brief	Display brief information about all module part of the device.
show system mpu [brief | *mpu-num*]	Display the MPU information.
show system power [*power-num* | brief]	Display the power supply information.
show tech-support { sys-base [detail] | drv-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.

2.7.3 Typical Configuration Example of System Management

2.7.3.1 Configure Login Limit Based on User and IP

Network Requirements

PC1 and PC2 serve as the local terminals, and can log into Device via telnet, ssh. Device can limit the login for PC1 and PC2 via the user and IP.

Network Topology

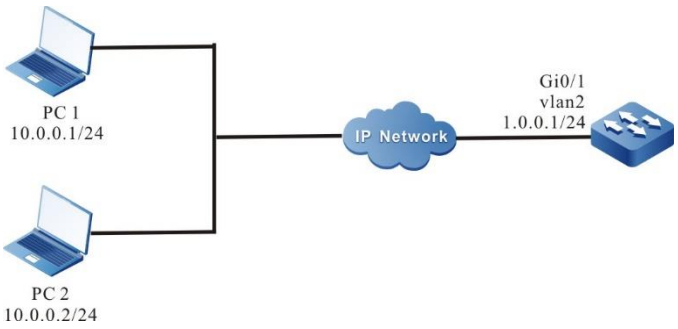


Figure 22 Networking for configuring the login limit based on the user, IP

Configuration Steps

Step 1: Configure the IP address of the interface, and configure the routing protocol to make PC1, PC2, and Device communicate with each other (omitted).

Step 2: Configure the login limit function based on the user, IP.

#Enable the telnet, ssh login security function.

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

#Configure the maximum try times of the telnet and ssh IP as 5 respectively, and the maximum try times of the user is 5.

```
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 ssh service of Device, configure the user name and password, and set using the local authentication login.

```
Device(config)#ip ssh server
Device(config)#local-user user1 class manager
```

```
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#password 0 admin
Device(config-user-manager-user1)#exit
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Check the result.

#PC1 tries to login to Device via telnet, and the user name is user1. After inputting the wrong password for successive 6 times, view the user information of the telnet login security statistics on Device:

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

You can see that user1 is regarded as the login attack user, and cannot log into the device via telnet within10 minutes.

Here, PC1 tries to use user1 to log into Device via telnet again, and the system prompts the login is prohibited.

#PC2 tries to log into Device via ssh, and uses the un-configured user name of Device. After logging in for successive 6 times, view the ip information of the ssh login security statistics:

```
Device#show login-secure ssh ip-addr
ssh module forbidden login address:
client address  try-time  forbid-time    type     number  record-time
--------------  -------- -----------  ------   ------ -----------
10.0.0.2      6       00:09:00       login    0      00:01:00
```

You can see that IP address of PC2 is regarded as the login attack user, and cannot log into the device via ssh within10 minutes.

Here, PC1 tries to log into Device via ssh again, and the system prompts the login is prohibited.

Note

- It is regarded as the login attack and is prohibited only after the login times exceeds the configured maximum retry times. When the login times is equal to the configured maximum times, it is not prohibited.
- Some ssh clients on the PC will retry inside after logging fails. In this case, the device is still recorded as multiple logins.
- By default, the device enables the telnetm ssh login security function.

2.7.3.2 Configure Fast Login Limit

Network Requirements

PC1 and PC2 serve as the local terminals, and can log into Device via telnet.

After PC1 fast logs into Device repeatedly, the login is limited, and PC2 is not affected.

Network Topology

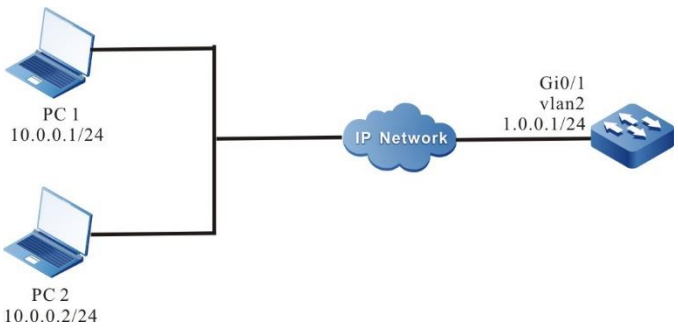


Figure 23 Networking for configuring the fast login limit

Configuration Steps

Step 1: Configure the IP address of the interface, and configure the routing protocol to make PC1, PC2, and Device communicate with each other (omitted).

Step 2: Configure the telnet fast login limit function.

#Enable telnet login security function, and configure the maximum fast login times as 20 and the prohibit time as 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 login user name and password of Device, and set using the local authentication login.

```
Device(config)#local-user user1 class manager
Device(config-user-manager-user1)#service-type ssh
Device(config-user-manager-user1)#password 0 admin
Device(config-user-manager-user1)#exit
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Check the result.

PC1 uses user1 to log in and log out repeatedly for 21 times via telnet, the login interval does not exceed 30s, and view the fast connection information of telnet login security statistics.

```
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
```

You can see that PC1 is regarded as the login attack address, and is not permitted to log into the device via telnet for 10 minutes.

PC2 can log into Device via telnet successfully.

2.8 System Alarm

2.8.1 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 switch chip or main board temperature reaches the threshold, abnormal system alarm log information is generated. By default, the switch chip alarm temperature threshold is 115° and the main board temperature alarm threshold is 115°. Power supply and fan exceptions also generate abnormal system alarm log information.

2.8.2 System Alarm Function Configuration

Table 76 System Alarm Function List

Configuration Tasks	
Configure system temperature alarms.	Configure system temperature alarms.
Configure the system CPU alarm	Configure the system CPU alarm
Configure the system memory alarm	Configure the system memory alarm
Configure system power supply alarms.	Configure system power supply alarms.
Configure system fan alarms.	Configure system fan alarms.

2.8.2.1 Configure System Temperature Alarms

Configuration Condition

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 for switch chip or mainboard alarms. If the switch chip or mainboard temperature reaches the threshold, system alarm log information is generated. By default, the switch chip alarm temperature threshold is 115° and the mainboard alarm temperature threshold is 115°.

Table 77 Configuring System Temperature Alarms

Step	Command	Description
Enter the global configuration mode.	config terminal	-
Configure the threshold for switch chip or mainboard temperature alarms.	alarm temperature mpu { switch | mainboard} *temperature*	Mandatory.
In the VST mode, configure the switch chip or mainboard temperature alarm threshold of one in-place virtual switch member device	alarm temperature device *device-num* mpu { switch| mainboard} *temperature*	Mandatory.

2.8.2.2 Configure System CPU Alarm

Configuration Condition

Before configuring the system alarm, first complete the following task:

- After the system is started and operates stably, all boards are loaded successfully.

Configure System CPU Alarm

Configuring the system CPU alarm indicates that after configuring the CPU utilization monitor threshold, generate the CPU utilization abnormal alarm when exceeding the monitor threshold.

Table 78 Configure the system CPU alarm

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

Step	Command	Description
Configure the system CPU utilization alarm threshold	cpu utilization warner-threashold [*rate-value*]	Optional

2.8.2.3 Configure Low Memory Usage Threshold

Configuration Conditions

Before configuring the system threshold alarm, first complete the following task:

- After the system is started and operates stably, all cards are loaded successfully.

Configure Low System Memory Usage Threshold

Configuring the low system memory usage threshold indicates that after configuring the low system memory usage threshold and the system memory is lower than the low threshold, enter the system shortage status.

Table 79 Configure the system memory threshold alarm

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the system memory threshold alarm	memory threshold low *low-value*	Optional By default, the low system memory threshold is 8M.

2.8.2.4 Configure System Memory Alarm

Configuration Condition

Before configuring the system alarm, first complete the following task:

- After the system is started and operates stably, all boards are loaded successfully.

Configure System Memory Alarm

Configuring the system memory alarm indicates that after configuring the system memory utilization monitor threshold, generate the system memory utilization abnormal alarm when exceeding the monitor threshold.

Table 80 Configure the system memory alarm

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

2.8.2.5 Configure System Power Supply Alarms

Configuration Condition

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.

2.8.2.6 Configure System Fan Alarms

Configuration Condition

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.

2.9 System Log Configuration

2.9.1 Overview

The 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 81 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.

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

Table 82 Log Output Directions

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

The log module runs in a separate syslog process. The main thread of the syslog process receives the log information sent by the system. Firstly, process the log data and distribute the cache space. Then, load the configured output actions to the corresponding buffer queue of each output terminal. Because of the length limitation of the cache queue, when a large number of log information is output, there is a loss of log information. At this time, the log module will count the lost messages. There are two threads in the output of log scheduling (when the log information is output to the console, monitor, log server, run in the same sub-thread as log files; when the log information is output to email, run in another sub-thread). In the scheduling thread, enable a timer for each output direction, and after responding each time, the timer gets the log information data from the queue corresponding to the terminal and outputs to the corresponding terminal according to the user configuration.

2.9.2 System Log Function Configuration

Table 83 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 log output to email

Configuration Tasks	
Configure the timestamp for logs.	Configure the timestamp for logs.
Configure the operation log to be sent to the log server	Configure the operation log to be sent to the log server
Configure the log repeat suppression function	Configure the log repeat suppression function
Configure the log file capacity.	Configure the log file capacity.
Configure the log file encryption function	Configure the log file encryption function
Configure log display colors.	Configure log display colors.
Configure the log filter function	Configure the log filter function
Configure device origin-id	Configure device origin-id

2.9.2.1 Configure Log Output Functions

Configuration Condition

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.

Table 84 Configuring Log Output to the Control 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 control console.	logging source { *module-name* | default } console { level *severity* | deny }	Optional. By default, log display on the control console is enabled.

Configure Log Output to the Monitor Console

The monitor console refers to the Telnet or SSH terminal. It is used for remote device management. To configure the log output to the monitor console, you need to

enable the log display on the current terminal.

Table 85 Configuring Log Output to the Monitor 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 source { *module-name* | default } monitor { level *severity* | deny }	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 record the log information in a more comprehensive manner, you can configure the log information output to the log server, which is convenient for the maintenance and management of the system. When configuring the log output to the log server, you need to configure the host address or domain name of the log server.

Table 86 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.
Configure the log output to the log server	logging server *server-name* [vrf *vrf-name*] { ip *ip-address* | ipv6 *ipv6-address* | hostname *host-name*} [port *port-num*] [	Mandatory By default, do not configure the log output to the log server.

Step	Command	Description
	facility *facility-name*] [level *severity*]	
Configure the IP source address for sending the log information	logging server source { ip *ip-address* | ipv6 *ipv6-address* | interface *interface-name* }	Optional By default, confirm the output interface of sending the log information by the route, and use the master IP address of the output interface as the source IP address of the sent log information.
Configure the log information of the specified level output to the log server	logging source { *module-name* | default } server [*server-name &<1-8>*] { level *severity* | deny }	Optional By default, the log information of level 0-5 can be output to the log host.

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 the log information from device syslog startup to the system restarting or before syslog process restarting. By default, log information of level 5 (notifications) and higher levels are stored. By default, the flash memory stores log information of level 5 (**notifications**) and higher levels. For the levels of logs, refer to the detailed description in Table 9-1. Both the two types of log files have capacity limit. If the size of log files reaches the configured maximum capacity, first delete the oldest log file (the log information is recorded by multiple log files) when adding one log, and then, add one log file and record the log information to the new log file.

Table 87 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

Step	Command	Description
		function is enabled.
Configure the log output to Flash	logging source { *module-name* | default } file { level *severity* | deny }	Optional By default, the log information of level 0-5 is saved to Flash.
Configure the log output to memory	logging source { *module-name* | default } buffer { level *severity* | deny }	Optional By default, the log information of level 0-5 is saved to memory.
Configure the log file capacity alarm	logging { buffer | file } warning warning-value recover-value	Optional By default, the log information warning value is 90%, and the recover value is 70%.
Configure the log file compression	logging compress [gunzip] logging compress max-num *value*	Optional By default, do not enable the log compression function.

Configure Log Output to Email

In order to record the log information more comprehensively, we can configure the log information to be output to the email box of the recipient and copier through email.

Table 88 Configuring Log Output to Email

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 the email profile	logging email email-profile	Mandatory By default, do not configure the profile of outputting the log to

Step	Command	Description
		email.
Configure the email address of the recipient of the log information	mail recipient mail-address	Mandatory By default, do not configure the email address of the recipient of the log information.
Configure the email address of the copier for receiving the log information	mail copyto mail-address	Optional By default, do not configure the email address of the copier for receiving the log information.
Configure the email address of the sender of the log information	mail sender mail-address	Mandatory By default, do not configure the email address of the sender of the log information.
Configure the email password of the sender of the log information	mail sender password *password-string*	Mandatory By default, do not configure the email password of the sender of the log information.
Configure the email domain name address of the receiver of the log information	mail server *server-name*	Optional By default, take the characters after the @ in the email address of the sender as the domain name address of the sender.
Configure the email subject of sending the log information	mail subject subject-name	Optional By default, do not configure the email subject of sending the log information.
Configure the log information of the specified level output to the email box of the receiver and copier via email	logging source { *module-name* | default } email { level *severity* | deny }	Optional By default, the log information of level 0-4 is output to email.

2.9.2.2 Configure the Timestamp for Logs

Configuration Condition

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 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.

Table 89 Configuring the Timestamp for Logs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the timestamp type of the log information	logging timestamps uptime	Optional By default, the log information adopt the absolute stamp type.
Configure the timestamp format for logs.	logging timestamp-format { msec | timezone | year }	Optional By default, the log information adopts the timestamp format with the year to display.

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.

2.9.2.3 Configure Operation Log Output to Log Host

Configuration Condition

You need to configure the log output to the host first.

Configure Operation Log Output to Log Server

After configuring the operation log output to the log server, you can query the operation log of the user on the log server.

Table 90 Configure the operation log output to the log host

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 the log host	logging server *server-name* [vrf *vrf-name*] { ip *ip-address* | ipv6 *ipv6-address* | hostname *host-name* } [port *port-num*] [facility *facility-name*] [level *severity*]	Mandatory By default, the function of sending the log information to the log server is not enabled.
Configure the operation log sent to the log server	logging operation to-server	Mandatory By default, the function of sending the operation log to the log server is not enabled.

2.9.2.4 Configure Log Repeat Suppression

Configuration Condition

None

Configure Log Repeat Information Suppression

In some cases, the module may continuously output the same log, affecting the observation of other logs. At this time, you can enable the repeat suppression function the log information. The repeated log information is output once in each suppression period, and the times that the log is suppressed in the suppression period is output at the end of the suppression period.

Table 91 Configure the log repeat suppression

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the suppression function of the log repeat information	logging suppress duplicates interval *interval-num*	Mandatory By default, the log suppression function is enabled.

2. 9. 2. 5 Configure the Log File Capacity

Configuration Condition

None

Configure the Log File Capacity

Limited by the capacity of the flash memory, the log file capacity can be configured from 1M-16M bytes. When the size of stored log information exceeds the maximum capacity limit, the new log overwrites the old log information (take the file as the unit to cover the old log information file).

Table 92 Configuring the Log File Capacity

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

2.9.2.6 Configure Log File Encryption

Configuration Condition

None

Configure Log File Capacity

Considering the security of log information, the log files stored in flash can be encrypted. When configuring the encryption function of log files, the subsequent

generated logs will be stored in the log file as ciphertext. If the password of log files changes, the previously stored logs in ciphertext will not be displayed in plaintext. The log information be stored in the form of plaintext only when the password is reconfigured as the password when the log is generated.

Table 93 Configure Log File Encryption

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the log file encryption	logging file encryption alogrithms SMV4 key password	Optional By default, do not configure the encryption function for the log file in Flash.

2.9.2.7 Configure Log Display Colors

Configuration Condition

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 94 Description of Log Colors

Field	Description
emergencies	Red
alerts	Purple
alerts	Blue
errors	Brown
warnings	Cyan
notifications	White
informational	Green

debugging	Green

Table 95 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.

2.9.2.8 Configure Log Filter Function

Configuration Condition

None

Configure Log Filter Function

When configuring log filtering, you can specify to display not only the log information containing the filter string, but also the log information without the filter string and the log information level range. When using this command, the filter string needs to be used together with the log level range.

Table 96 Configure the log filter function

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Configure the log filter function	logging filter { exclude *exclude-string* | include *include-string* | level *high-level low-level* }	Optional By default, the log filter function is not enabled.

2.9.2.9 Configure Device origin-id

Configuration Condition

None

Configure Device origin-id

When configuring the device origin-id, support max. 63 characters. After configuring the origin-id, the hostname field of the log sent to the log server will be replaced by the origin-id string.

Table 97 Configure device origin-id

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure device origin-id	logging origin-id string *origin-id*	Optional By default, do not configure the device origin-id.

2.9.2.10 Log Monitoring and Maintaining

Table 98 Log Monitoring and Maintaining

Command	Description
clear logging [buffer | file]	Clear the log information stored in memory or Flash
show logging [buffer | file]	Display the log information that is stored in the memory or flash memory.
show logging { file | buffer } desc	Reversely display the log information stored in the memory or Flash
show logging filter	Display the log filtering configuration information
show logging operation	Display the log information stored in the operation log

Command	Description
	file
show logging [{ file | buffer } [begin-level *level-value* / [start-time *stime* [end-time *etime*]] [detail]]]	Display the log information stored in log files, filtering to display the log information with the time and level filtering option
show logging { file | buffer } message-counter	Display the size of the log file and the number of the log information entries stored in Flash or memory.

2.10 Software Upgrade

2.10.1 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/SFTP network transmission mode, specified local directory 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: The program package of the main board 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.

- **FPGA (Field Programmade Gate Array)** program: the program with suffix bin, which is mainly used to realize the logic control of devices and the sending and receiving of service data.
- The Bootloader program: The program with the suffix .bin or. pck, the boatloader program of the main control board, fixed in the ROM of the main control board and the main board of the business board, is executed first after the device is powered on. This program initializes the basic system, and its main function is to guide the operating system to load.
- **Devinfo**: OEM program, including model ID and function ID of various devices and boards. It is mainly used for upgrading when the device is modified.
- **Patch**: Hot patch is a fast and low-cost way to repair defects in product software versions. Compared with upgrading the software version, the main advantage of hot patch is that it will not interrupt the current running business of the device, that is, it can repair the defects of the current software version of the device without restarting the device.
- **Feature**: The feature incremental package is a fast and low-cost way to repair product software version defects. It can replace the business process program file and dynamic library program file in the software version. After the business process program file is replaced, it will automatically restart and take effect, and the dynamic library program file will take effect after restarting the device. Compared with upgrading the software version, the main advantage of upgrading the business process program file is that it will not interrupt the current running business of the device for a long time, that is, the defects of the current software version of the device can be repaired without restarting the device; The upgrade time of dynamic library program

files is relatively short, which can quickly complete version replacement and defect repair.

- **Package program**: The package file with the image, Bootloader, cmm, devinfo program, which can upgrade various types of software programs once.
- **ISSU** (In-Service Software Upgrade): Uninterrupted service version upgrade is an upgrade method to ensure uninterrupted service or short interruption time during the upgrade process. ISSU related functions are used to upgrade the version of the key device in key network environments (such as data center) without interrupting business traffic. The premise of ISSU upgrade is that the device has backup. Previously, the download of the new version of the program has been completed through sysupdate related commands.

The applicable relationship between the above types of upgrade software and each type of board card is shown in the table:

Table 99 Applicable relationship between upgrade programs and boards

	image program package	bootload program	devinfo file	patch file	feature file	package package file	ISSU
Main control board	√	√	√	√	√	√	√

2.10.2 Software Upgrade Function Configuration

Table 100 Software Upgrade Function List

Configuration Tasks	
Upgrade the image program package.	Upgrade the image program package of the main control board in TFTP/FTP/SFTP/local upgrade mode.
Upgrade the Bootloader program.	Upgrade the Bootloader program in TFTP/FTP/SFTP/local upgrade mode.
Upgrade the devinfo file	Upgrade the devinfo file package in TFTP/FTP/SFTP/local upgrade mode.

Configuration Tasks	
Upgrade the patch file	Upgrade the hot patch in TFTP/FTP/SFTP/local upgrade mode.
Upgrade the feature file	Upgrade the feature incremental package in TFTP/FTP/SFTP/local upgrade mode.
Upgrade the package program.	Upgrade the package program via the TFTP/FTP/SFTP mode
Upgrade ISSU	Upgrade the version program without interrupting business traffic or interrupting business traffic for a short time

2.10.2.1 Upgrade the image Program Package

The image program package is used to upgrade the main control board.

Configuration Preparations

Before upgrading the image program package, ensure that:

- The route between the TFTP/FTP/SFTP server and the device interface is reachable, and the TFTP/FTP/SFTP server and the device can ping each other successfully.
- The TFTP/FTP/SFTP server configuration is correct, and the image program is stored in the specified directory of the TFTP/FTP/SFTP server.
- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory of storage devices such as USB.
- The remaining space of the flash is sufficient. If the space is insufficient, manually delete the unnecessary files in the flash.
- The configuration files have been backed up.

Upgrade the image Program Package in TFTP/FTP/SFTP/Local Upgrade Mode

Enter the privileged user mode, ensure that the device can obtain the upgrade

program through the external TFTP/FTP/SFTP server, and then use the **sysupdate image** command to upgrade the program package.

Table 101 Upgrading the image Program Package in TFTP/FTP/SFTP/local upgrade Mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the image program package.	sysupdate image [device { memberId | all }] mpu {file-system filename | [vrf vrf-name] {dest-ip-address | dest-ipv6-address} filename [ftp | sftp username password]} [reload]	Mandatory. If the FTP/SFTP option is not specified, TFTP is used for upgrade by default.

Example: In the standalone mode, make use of the FTP server 130.255.168.45 to upgrade the image program package of the online control board.

```
Hostname#sysupdate image mpu 130.255.168.45 sp35-g-9.7.20.1(R).pck ftp a a
```

#The device gives the following prompt messages:

```
checking "sp35-g-9.7.20.1(R).pck" : ...OK
downloading "sp35-g-9.7.20.1(R).pck" :
########################################OK
Download "sp35-g-9.7.20.1(R).pck" (177498836 Bytes) successfully.
Verify the image...valid
Writing file to filesystem.....OK!
Start backup ios to raw flash...OK
 %Sysupdate image is in process, please wait...
 %Sysupdate image finished.

     sysupdate image result information list:
-------------------------------------------------------------
     Card      result information
-------------------------------------------------------------
     Mpu       upgrade successfully!
```

Example: In standalone mode, upgrade the image program of the main control board through file-system.

```
Hostname#sysupdate image mpu file-system /flash/sp35-g-9.7.20.1(R).pck
```

#The device gives the following prompt messages:

```
checking "/flash/ sp35-g-9.7.20.1(R).pck" : ...OK
Copying "/flash/ sp35-g-9.7.20.1(R).pck" :
########################################OK
Copy "/flash/ sp35-g-9.7.20.1(R).pck" (177498836 Bytes) successfully.
Verify the image...valid
Writing file to filesystem.....OK
Start backup ios to raw flash.....OK
 %Sysupdate image is in process, please wait...
%Sysupdate image finished.

     sysupdate image result information list:
----------------------------------------------------------------
     Card      result information
----------------------------------------------------------------
     Mpu 0     upgrade successfully.
```

#The above message indicates that the image program of the online active and standby control cards have 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. 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 remaining space in the flash. If the space is insufficient, the upgrade fails. In this case, you can manually delete files that are not in need from the flash to obtain more space for upgrading application programs.
- When the flash space of the active and standby control cards is insufficient, it will prompt whether to delete the redundant image files. If the space is still insufficient after deleting, the upgrade fails.
- It takes a long time to upgrade the image program package. A smaller

remaining space in the flash 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, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the flash file system of the main control board may be damaged.

2.10.2.2 Upgrade the Bootloader Program

The Bootloader program is used to upgrade the main control card.

Configuration Preparations

Before upgrading the Bootloader program, ensure that:

- The route between the TFTP/FTP/SFTP server and the device interface is reachable, and the TFTP/FTP/SFTP server and the device can ping each other successfully.
- The TFTP/FTP/SFTP server configuration is correct, and the Bootloader program is stored in the specified directory of the TFTP/FTP/SFTP server.
- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory

of storage devices such as USB.

- Back up the configuration file.

Upgrade the Bootloader Program in TFTP/FTP/SFTP/Local Upgrade Mode Mode

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

Table 102 Upgrading the Bootloader program in TFTP/FTP/SFTP/local upgrade mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the Bootloader program.	sysupdate bootloader [device { *memberId* | all }] mpu {file-system *filename* | [vrf *vrf-name*] {*dest-ip-address* | *dest-ipv6-address*} *filename* [ftp | sftp *username password*]} [reload]	Mandatory. If the FTP/SFTP option is not specified, TFTP is used for upgrade by default.

Example:

In the standalone mode, make use of FTP server 130.255.168.45 to upgrade the bootloader program of all online main control boards.

```
Hostname#sysupdate bootloader mpu 130.255.168.45 sz03-tboots2-b6b7-9.6.2.5.pck ftp a a
```

#The device will prompt the following information:

```
checking " sz03-tboots2-b6b7-9.6.2.5.pck " : ...OK
downloading " sz03-tboots2-b6b7-9.6.2.5.pck" : ####OK
Download " sz03-tboots2-b6b7-9.6.2.5.pck " (3637108 Bytes) successfully.
Update bootloader start.
.....OK.

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

```
    sysupdate bootloader result information list:
---------------------------------------------------------------
    Card      result information
---------------------------------------------------------------
    Mpu     upgrade successfully!
```

#The above message indicates that the Bootloader program of the online main control card has been upgraded successfully.

Example: In the stand-alone mode, the local upgrade is performed through file-system to upgrade the bootloader programs of all the existing main control boards.

```
Hostname#sysupdate bootloader mpu file-system /flash/sz03-tboots2-b6b7-9.6.2.5.pck
```

#The device will prompt the following information:

```
checking "/flash/sz03-tboots2-b6b7-9.6.2.5.pck " : ...OK
Copying "/flash/sz03-tboots2-b6b7-9.6.2.5.pck" : ####OK
Copy "/flash/sz03-tboots2-b6b7-9.6.2.5.pck " (3637108 Bytes) successfully.
Update bootloader start.
.....OK.

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

    sysupdate bootloader result information list:
---------------------------------------------------------------
    Card      result information
---------------------------------------------------------------
    Mpu     upgrade successfully!
```

Note

- When upgrading, please select the correct version of Bootloader to avoid abnormal situation.
- If the command option reload is added, the system prompts whether to save

the configuration, and whether to restart the device immediately. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.

- After upgrading is complete, if you need to run a new bootloader program, you need to restart the board or the whole device.
- Please select the correct bootloader version to upgrade to avoid abnormality.

Warning

- During the upgrade process, you cannot power off the device or swap or restart the main control board and service card. Otherwise, the system may fail to start, or the Bootloader file of the board card may be damaged.

Upgrade the Bootloader Program via the Console Port

Ensure that the HyperTerminal can access the device through the Console port. Enter the Bootloader mode, adjust the baud rate, and perform the upgrade through the ymodem of the HyperTerminal. If there are two master cards on the device, you need to upgrade them separately.

For details of the commands, refer to the related chapter of the “Bootloader” command manual.

Table 103 Upgrading the Bootloader Program via the Console Port

Step	Command	Description
Set the HyperTerminal.	None	Mandatory. Run the HyperTerminal program, select the corresponding serial port (such as com1) and set its properties. Set baud rate to 9600 bps, soft flow control, 8 data bits, no parity check, and 1 stop bit.

Step	Command	Description
Enter the Bootloader mode.	None	Mandatory. When the device restarts, press Ctrl + C to enter the Bootloader mode.
Modify the baud rate of the Console port and HyperTerminal to improve the upgrade speed.	srate { *speed* }	Optional. Modify the baud rate of the device Console port to 115200 bps. Then, disconnect the HyperTerminal, and modify the baud rate of the HyperTerminal to 115200 bps, and then connect the HyperTerminal again.
Upgrade the Bootloader program.	mupdate Bootloader	Mandatory. In the Bootloader mode, input the mupdate Bootloader command, select the ymodem protocol of the HyperTerminal, and select the Bootloader program to start transmission.

Example:

The following example shows how to upgrade the Bootloader program of the active control card through the Console port.

#The device gives the following prompt messages:

```
PMON> mupdate bootloader
download bootloader via y modem protocol.....CCC
Starting ymodem transfer.  Press Ctrl+C to cancel.
Transferring sz03-tboots2-b6b7-9.6.2.5.pck...
  100%    1020 KB      7 KB/sec    00:02:24       0 Errors
## Total Size      = 0x000ff0f4 = 1044724 Bytes
 success!
Update bootloader start...
Erase Master Flash OK ...
-Flash Program OK ...
Verifying flash data...
```

```
Verify OK ...
Update bootloader OK.
PMON>
```

#The above message indicates that the bootloader program of the active control card has been upgraded successfully.

Note

- When upgrading the bootloader program of the standby control card through the console port, the operation process is consistent with that of the active control card.
- In upgrading the Bootloader program, ensure that the rate of the HyperTerminal is the same as the rate of the device Console port.
- In upgrading the Bootloader program, the transmission speed is recommended to be set to 115200 bps. In this way, the upgrade transmission time is shorter.
- 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 9600bps. At this time, the rate of the HyperTerminal needs to be modified synchronously.
- It is recommended that you upgrade the Bootloader program in TFTP/FTP/SFTP mode. The Console port upgrade mode is used only when the upgrade conditions of the first upgrade mode fail to be satisfied.

Warning

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or

the Bootloader file of the board card may be damaged.

2.10.2.3 Upgrade the devinfo File

The devinfo file is used to upgrade the main control board.

Configuration Preparations

Before upgrading the devinfo file, ensure that:

- The route between the TFTP/FTP/SFTP server and the device interface is reachable, and the TFTP/FTP/SFTP server and the device can ping each other successfully.
- The TFTP/FTP/SFTP server configuration is correct, and the devinfo file is stored in the specified directory of the TFTP/FTP/SFTP server.
- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory of storage devices such as USB.
- Back up the configuration file.

Upgrade the devinfo File in TFTP/FTP/SFTP/Local Upgrade Mode

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

Table 104 Upgrading the devinfo file in TFTP/FTP/SFTP /local upgrade mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the devinfo file	sysupdate devinfo [device { memberId | all }] mpu {file-system filename | {dest-ip-address | dest-ipv6-address} filename [ftp | sftp username password]} [reload]	Mandatory If the FTP/SFTP option is not specified, TFTP is used for upgrade by default.

Example:

In the standalone mode, make use of FTP server 130.255.168.45 to upgrade the devinfo files of the online main control board.

```
Hostname#sysupdate devinfo mpu 130.255.168.45 devInfo_sw_SOFINET_V2.155 ftp a a
```

#The device gives the following prompt messages:

```
checking " devInfo_sw_SOFINET_V2.155" : ...OK
downloading " devInfo_sw_SOFINET_V2.155" : #OK
Download " devInfo_sw_SOFINET_V2.155" (6275 Bytes) successfully.
Writing file to filesystem....OK!

 %Sysupdate devinfo is in process, please wait...
 %Sysupdate devinfo finished.

     sysupdate devinfo result information list:
---------------------------------------------------------------
     Card      result information
---------------------------------------------------------------
     Mpu       upgrade successfully!
```

Example: In the stand-alone mode, the local upgrade is carried out through file-system to upgrade the devinfo file of the online main control board.

```
Hostname#sysupdate devinfo mpu file-system /flash/devInfo_sw_SOFINET_V2.155
#The device gives the following prompt messages:
checking "/flash/devInfo_sw_SOFINET_V2.155" : ...OK
Copying "/flash/devInfo_sw_SOFINET_V2.155" : #OK
Copy "/flash/devInfo_sw_SOFINET_V2.155" (6275 Bytes) successfully.
Writing file to filesystem....OK!

 %Sysupdate devinfo is in process, please wait...
 %Sysupdate devinfo finished.

        sysupdate devinfo result information list:
---------------------------------------------------------------
        Card       result information
---------------------------------------------------------------
        Mpu        upgrade successfully!
```

#The above message indicates that the devinfo file of the online main control card

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. Usually, the device is started after all programs are upgraded. Therefore, the reload option is not recommended.
- After the upgrade is completed, to run the new devinfo file, restart the device.
- Select the correct devinfo file version to upgrade to avoid exceptions.

Warning

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the devinfo file may be damaged.

2.10.2.4 Upgrade the patch File

The patch file is applicable to upgrade the main control board.

Configuration Preparations

Before upgrading the patch file, ensure that:

- The route between the TFTP/FTP/SFTP server and the device interface is reachable, and the TFTP/FTP/SFTP server and the device can ping each other successfully.
- The TFTP/FTP/SFTP server configuration is correct, and the patch file is

stored in the specified directory of the TFTP/FTP/SFTP server.

- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory of storage devices such as USB.
- Back up the configuration file.

Upgrade the patch File in TFTP/FTP/SFTP/Local Upgrade Mode

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

Table 105 Upgrading the patch file in TFTP/FTP/SFTP /local upgrade mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the patch file	sysupdate patch [device { *memberId* | all }] mpu {file-system *filename* | [vrf *vrf-name*] {*dest-ip-address* | *dest-ipv6-address*} *filename* [ftp | sftp *username password*]}	Mandatory If the FTP/SFTP option is not specified, TFTP is used for upgrade by default.

Example:

In the standalone mode, make use of FTP server 130.255.168.45 to upgrade the patch files of the online main control board.

```
Hostname#sysupdate patch  mpu 130.255.168.45 sp35-g-9.7.20.1.HP001.pat ftp a 123456
downloading " sp35-g-9.7.20.1.HP001.pat" : #OK
Download " sp35-g-9.7.20.1.HP001.pat" (8693 Bytes) successfully.
Writing file to filesystem.....OK
Upgrading, please wait for a moment...
Load the patch package successfully.
Active the patch package successfully.
Run the patch package successfully.
Upgrade the patch package finished.
Upgrade patch of master MPU:OK
```

```
%Sysupdate patch is in process, please wait...
%Sysupdate patch finished.
      sysupdate patch result information list:
----------------------------------------------------------------
      Card    result information
----------------------------------------------------------------
      Mpu 0   upgrade successfully!
```

Example: In the stand-alone mode, the local upgrade is carried out through file-system to upgrade the patch file of the online main control board.

```
Hostname#sysupdate patch  mpu file-system /flash/sp35-g-9.7.20.1.HP001.pat
Copying "/flash/sp35-g-9.7.20.1.HP001.pat" : #OK
Copy "/flash/sp35-g-9.7.20.1.HP001.pat" (8693 Bytes) successfully.
Writing file to filesystem.....OK
Upgrading, please wait for a moment...
Load the patch package successfully.
Active the patch package successfully.
Run the patch package successfully.
Upgrade the patch package finished.
Upgrade patch of master MPU:OK
 %Sysupdate patch is in process, please wait...
 %Sysupdate patch finished.
      sysupdate patch result information list:
----------------------------------------------------------------
      Card    result information
----------------------------------------------------------------
      Mpu 0   upgrade successfully!
```

#The above information indicates that the patch file of the online control card has been upgraded successfully. You can view the successful patching through Hotpatch Version in show version. The version number is the version number of the patch file.

Note

- After the upgrade, the patch file will take effect immediately.
- Please select the correct patch file version to upgrade to avoid exceptions.

Warning

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the patch file may be damaged.

Delete patch Package

Enter the privileged user mode, and then delete the hot patch package through the **patch delete** command.

Table 106 Delete the hot patch package via the patch delete command

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Delete the hot patch package	patch delete [device { *memberId* | all }] mpu	Mandatory

Example: In the standalone mode, delete the hot patch package via the **patch delete** command.

```
Hostname#patch delete
This will delete the package. Are you sure?(Yes|No)?yes
Package deleting, please wait for a moment...
Rollback the patch package successfully.
Delete the patch package file successfully.
```

#The above information indicates that the patch package of the control card is deleted successfully, and the hot patch is no longer effective.

Note

- After deletion, the hot patch package will be deleted
- Please confirm clearly before executing this command. After execution, the hot patch will be invalid to avoid exceptions.

Patch Upgrade Monitoring and Maintaining

Table 107 patch upgrade monitoring and maintaining

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Display the installation and operation information of the patch package	show patch [device { *memberId* | all }] mpu	Display the information about the hot patch installation files and versions
Debug the installation process of the patch package	[no] debug hpmm	Debug the installation process of the hot patch package

2.10.2.5 Upgrade the feature File

The feature file is applicable to upgrade the control card.

Configuration Preparations

Before upgrading the feature file, ensure that:

- The route between the TFTP/FTP/SFTP server and the device interface is reachable, and the TFTP/FTP/SFTP server and the device can ping each other successfully.
- The TFTP/FTP/SFTP server configuration is correct, and the feature file is stored in the specified directory of the TFTP/FTP/SFTP server.
- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory of storage devices such as USB.
- Back up the configuration file.

Upgrade the feature File in TFTP/FTP/SFTP/Local Upgrade Mode

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

Table 108 Upgrading the feature file in TFTP/FTP/SFTP /local upgrade mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the feature file	sysupdate feature [device { *memberId* | all }] mpu {file-system *filename* | [vrf *vrf-name*] {*dest-ip-address* | *dest-ipv6-address*} *filename* [ftp | sftp *username password*] }	If the FTP/SFTP option is not specified, TFTP is used for upgrade by default.

Example: In the standalone mode, make use of FTP server 130.255.168.45 to upgrade the feature file of the online main control board.

```
Hostname#sysupdate feature mpu 130.255.168.45 sp35-g-9.7.20.1.FEATURE001.bin ftp a 123456
downloading " sp35-g-9.7.20.1.FEATURE001.bin " : #OK
Download " sp35-g-9.7.20.1.FEATURE001.bin " (9657 Bytes) successfully.
Writing file to filesystem.....OK
Upgrading, please wait for a moment...
Load the feature package successfully.
Active the feature package successfully.
Run the feature package successfully.
Upgrade the feature package finished.
Upgrade feature of master MPU:OK
 %Sysupdate feature is in process, please wait...
 %Sysupdate feature finished.
      sysupdate feature result information list:
---------------------------------------------------------------
      Card    result information
---------------------------------------------------------------
      Mpu 0   upgrade successfully!
```

Example: In the stand-alone mode, the local upgrade is carried out through file-system to upgrade the feature file of the online main control board.

```
Hostname#sysupdate feature mpu file-system /flash/sp35-g-9.7.20.1.FEATURE001.bin
```

```
Copying "/flash/sp35-g-9.7.20.1.FEATURE001.bin " : #OK
Copy "/flash/sp35-g-9.7.20.1.FEATURE001.bin " (9657 Bytes) successfully.
Writing file to filesystem.....OK
Upgrading, please wait for a moment...
Load the feature package successfully.
Active the feature package successfully.
Run the feature package successfully.
Upgrade the feature package finished.
Upgrade feature of master MPU:OK
 %Sysupdate feature is in process, please wait...
 %Sysupdate feature finished.
      sysupdate feature result information list:
-------------------------------------------------------------------
      Card    result information
-------------------------------------------------------------------
      Mpu 0   upgrade successfully!
```

#The above information indicates that the feature file of the online control card has been upgraded successfully. You can view the successful patching through Feature Version in show version. The version number is the version number of the patch file.

Note

- After the upgrade, the business process program file in the feature file will automatically take effect immediately, and the dynamic library program file will take effect after the system is restarted.
- Please select the correct feature file version to upgrade to avoid exceptions.

Warning

- During the upgrade process, you cannot power off the device or swap or restart the main control board. Otherwise, the system may fail to start, or the feature file may be damaged.

Delete feature Incremental Package

Enter the privileged user mode, and then delete the feature increment package through the **feature delete** command.

Table 109 Delete the feature increment package through the feature delete command

Step	Command	Description
Enter the privileged user mode.	None	Mandatory
Delete the feature increment package	feature delete [device { *memberId* | all }] mpu	Mandatory

Example: In the standalone mode, delete the feature increment package via the **feature delete** command.

```
Hostname#feature delete
This will delete the package. Are you sure?(Yes|No)?yes
Package deleting, please wait for a moment...
Rollback the feature package successfully.
Delete the feature package file successfully.
```

#The above information indicates that the feature incremental package of the control card is deleted successfully, and the feature incremental package is no longer effective.

Note

- When the deletion is complete, the feature incremental package is deleted.
- Please confirm clearly before executing this command to avoid exceptions. After execution, the corresponding business process in the package will automatically restart with the old business process program file. The dynamic library program file will resume to use the old after restarting the device, that is, the previously upgraded business process program file will automatically become invalid, and the dynamic library program file will become invalid after restarting the device.

Feature Upgrade Monitoring and Maintaining

Table 110 feature upgrade monitoring and maintaining

Step	Command	Description
Enter the privileged user mode.	None	Mandatory.
Display the installation and operation information of the feature incremental package	show feature [device { *memberId* | all }] mpu	Display the information about the feature incremental package installation files and versions
Debug the installation process of the feature incremental package	[no] debug hpmm	Debug the installation process of the feature incremental package

2.10.2.6 Upgrade the Package File

The package file contains the image, bootloader files, which can be upgraded once via the package file.

Configuration Preparations

Before upgrading the package file, you need to complete the following task:

- Ensure that the route between the TFTP/FTP/SFTP server and the device interface is reachable, and they can ping each other.
- The TFTP/FTP/SFTP server is configured correctly, and the package file is correctly placed in the specified directory of TFTP/FTP/SFTP.
- When upgrading through local upgrade, you need to ensure that the version is in the specified directory. You can specify the version file in the directory of storage devices such as USB.

- Back up the configuration file.

Upgrade Package File via TFTP/FTP/SFTP/Local Upgrade Mode

Enter the privileged user mode, ensure that the device can get the upgrade program from the external TFTP/FTP/SFTP server, and then, upgrade via the **sysupdate package** command.

Table 111 Upgrade the package file via TFTP/FTP/SFTP/local upgrade mode

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Upgrade the package file	sysupdate package [device { *memberId* | all }] {file-system *filename* | [vrf *vrf-name*] {*dest-ip-address* | *dest-ipv6-address*} *filename*[ftp | sftp *username password*]} [no-comparision] [reload]	Mandatory If not specifying the FTP option, use TFTP to upgrade by default.

Example: In the standalone mode, package and upgrade the programs of all types of online boards through FTP server 130.255.168.45.

```
Hostname#sysupdate package 130.255.168.45 sp35-g-9.7.20.1(R)-001.pkg FTP a a
```

#The device prompts the following information:

```
Downloading "sp35-g-9.7.20.1(R)-001.pkg" header...OK!
Checking "sp35-g-9.7.20.1(R)-001.pkg" header...OK!


     image file version comparision:
-----------------------------------------------------------------
Component        Component version      File version
-----------------------------------------------------------------
Mpu 0            9.7.20.1(R)            9.7.20.1(R)

The current-version of cards is greater than or equal to that in package.

NOTICE:input 'Yes' to upgrade all files in the package, 'No' to ignore the above component(s).
(Yes|No)?Yes

Downloading                          "sp35-g-9.7.20.1(R)-001.pkg"                          :
##################################################################
##################################################################
```

```
##############################################OK!
Download "sp35-g-9.7.20.1(R)-001.pkg" (181635232 Bytes) successfully!
Checking package file...OK!
Verify the image...valid
The file sp35-g-9.7.20.1(R).pck already exists on Mpu 0, overwrite it?(Yes|No):Yes
Writing file to filesystem.....OK!
Start backup ios to raw flash...OK
 %Sysupdate image is in process, please wait...
 %Sysupdate image finished.
Update bootloader start.
...OK.
 %Sysupdate bootloader is in process, please wait...
 %Sysupdate bootloader finished..
%Sysupdate devinfo is in process, please wait...
 %Sysupdate devinfo finished..
 %Sysupdate pkgInfo is in process, please wait...
 %Sysupdate pkgInfo finished.

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

sp35-g-9.7.20.1(R).pck sysupdate result information list:
-----------------------------------------------------------------
      Mpu 0   -  upgrade successfully!

sz03-tboots2-b6b7-9.6.2.5.pck sysupdate result information list:
-----------------------------------------------------------------
      Mpu 0   -  upgrade successfully!

devInfo_sw_SOFINET_V2.155 sysupdate result information list:
-----------------------------------------------------------------
      Mpu 0   -  upgrade successfully!

pkg_info.txt sysupdate result information list:
-----------------------------------------------------------------
      Mpu 0   -  upgrade successfully!
```

Example: In the stand-alone mode, perform the local upgrade through the file system, and package and upgrade the programs of all types of online boards.

```
Hostname#sysupdate package 130.255.168.45 sp35-g-9.7.20.1(R)-001.pkg
```

#The device prompts the following information:

```
Downloading "sp35-g-9.7.20.1(R)-001.pkg" header...OK!
Checking "sp35-g-9.7.20.1(R)-001.pkg" header...OK!

      image file version comparision:
------------------------------------------------------------------
Component          Component version       File version
------------------------------------------------------------------
Mpu 0              9.7.20.1(R)             9.7.20.1(R)

The current-version of cards is greater than or equal to that in package.

NOTICE:input 'Yes' to upgrade all files in the package, 'No' to ignore the above component(s).
(Yes|No)?Yes

Copying                                "sp35-g-9.7.20.1(R)-001.pkg"                                :
##################################################OK!
Copy "sp35-g-9.7.20.1(R)-001.pkg" (181635232 Bytes) successfully!
Checking package file...OK!
Verify the image...valid
The file sp35-g-9.7.20.1(R).pck already exists on Mpu 0, overwrite it?(Yes|No):Yes
Writing file to filesystem.....OK!
Start backup ios to raw flash...OK
 %Sysupdate image is in process, please wait...
 %Sysupdate image finished.
Update bootloader start.
...OK.
 %Sysupdate bootloader is in process, please wait...
 %Sysupdate bootloader finished..
%Sysupdate devinfo is in process, please wait...
 %Sysupdate devinfo finished..
 %Sysupdate pkgInfo is in process, please wait...
 %Sysupdate pkgInfo finished.

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

sp35-g-9.7.20.1(R).pck sysupdate result information list:
------------------------------------------------------------------
```

```
    Mpu 0   -  upgrade successfully!

sz03-tboots2-b6b7-9.6.2.5.pck sysupdate result information list:
---------------------------------------------------------------
    Mpu 0   -  upgrade successfully!

devInfo_sw_SOFINET_V2.155 sysupdate result information list:
---------------------------------------------------------------
    Mpu 0   -  upgrade successfully!

pkg_info.txt sysupdate result information list:
---------------------------------------------------------------
    Mpu 0   -  upgrade successfully!
```

#The above information indicates that the packaged files of all types of online boards are upgraded successfully.

Note

- If the command option reload is added, the system prompts whether to save the configuration, and whether to restart the device immediately. However, usually the device is started after all programs are upgraded. Therefore, the reload option is not recommended.

Warning

- During the upgrade process, the device must not be powered off. Otherwise, the system may fail to start, or the file may be damaged.

2.10.2.7 Upgrade ISSU

ISSU is used to complete the device version program upgrade without interrupting business traffic or with interrupting service traffic for a short time.

Related Command Steps

Enter the privileged user mode and complete the upgrade without interrupting business traffic through the ISSU series commands.

Table 112 issu series operation commands

Step	Command	Description
Enter the privileged user mode.	enable	Mandatory.
Switch the business traffic of the standby device to the active device.	issu start	Mandatory The stacking scenario executes this command on the active device, and the MLAG and stand-alone backup scenario execute this command on the standby device.
Switch back the business traffic of the standby device	issu switchback	Mandatory Execute the command on the standby device.
Switch the service traffic of the active device to the standby device	issu switchover	Mandatory Execute the command on the active device.
Switch back the business traffic of the active device	issu switchback	Mandatory The stacking scenario executes this command on the original standby device, and the MLAG and stand-alone backup scenarios execute this command on the active device.

Warning

- Ensure that the device cannot be powered off during the upgrade process.
- Strictly follow the upgrade process. Otherwise, the packet loss time of the service traffic may exceed the requirements.

2.10.2.8 Software Upgrade Monitoring and Maintaining

Table 113 Software upgrade monitoring and maintaining

Command	Description
show issu	Display whether the current device is in the issu upgrade state.

2.10.3 Typical Configuration Example of Software Upgrade

2.10.3.1 Upgrade Package File

Network Requirements

- A PC acts as an FTP server, and Device acts as an FTP client. The network between the server and the client is normal.
- On the FTP server, set the user name for a device to log in to the FTP server as admin, and the password as admin. Place the package program to be upgraded in the FTP server directory, and upgrade all software versions of the device that support the package upgrading.

Network Topology

Figure 24 Networking for Upgrading all Supported Software Versions in Package

Configuration Steps

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

Step 2: Back up the device configuration file. (omitted)

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

Step 4: Upgrade the package upgrade program.

#Use sysupdate to upgrade the package upgrade program.

```
Device#sysupdate package 2.0.1.1 sp35-g-9.7.1.1(R)-001.pkg  ftp admin admin no-comparision
```

After the upgrade is completed, a list of upgrade results will be printed for users to determine the upgrade results of all upgrade programs included in the package

upgrade file on the device:

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

sp35-g-9.7.20.1(R).pck sysupdate result information list:
```

Warning

- Before upgrading in package, ensure that all cards are in place and the status is Start OK. During upgrading, do not swap the card, avoiding that the abnormal upgrading of the card affects the subsequent starting of the card.

```
    Mpu 0   -  upgrade successfully!

sz03-tboots2-b6b7-9.6.2.5.pck sysupdate result information list:
-----------------------------------------------------------------
    Mpu 0   -  upgrade successfully!

pkg_info.txt sysupdate result information list:
-----------------------------------------------------------------
    Mpu 0   -  upgrade successfully!
```

Note

- If selecting the "no-comparison" parameter, upgrade the version of the packaged upgrade program directly without image version comparison. If this parameter is not selected, the image version will be compared. If the image version in the packaged upgrade program is lower than the version running on the device or the same as the running version of the device, the device will prompt the user and wait for the user to confirm whether to upgrade the image upgrade program in the package. Whether the user chooses to upgrade the program or not will not affect the upgrade of the other upgrade files in the upgrade package. If there is only the image file in the packaged upgrade package, and the user chooses not to upgrade, the packaged upgrade ends.
- This command can also be added with a "reload" parameter. If the parameter is added, restart the device directly after the upgrade is completed.

Step 5: Use the command to restart the device.

#Use the reload command to restart the device.

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

Before restarting, whether to save the configuration depends on the actual needs of the user.

Note

- If the upgrade command
- contains the “reload” parameter, omit the step.

Step 6: Check the result.

#After completing the upgrade and restarting the device, query the upgraded file version information in the packaged upgrade program via the **show package version** command.

```
Device # show package version

package       :sp35-g-9.7.20.1(R)-001.pkg
image         :sp35-g-9.7.20.1(R).pck
bootloader    :sz03-tboots2-b6b7-9.6.2.5.pck
```

#Query the version number of the program via the **show system version brief** command to check whether it is updated.

```
Device #show system version  brief

version information display:

Module    Online State     Name                BootLoader  IOS             CMM     PCB
CPLD   FPGA
-------------------------------------------------------------------------------------
----------------------------------------
Mpu 0     online Start Ok   SOFOS SFN3300       9.6.2.5   9.7.20.1 (integrity)   /      001   /
/
```

Warning

- Query the version of the upgrade file in the packaged upgrade program via the show package version command, and query the final upgrade result via the show system version brief command.

2.10.3.2 Upgrade All Software Versions

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. Upgrade all software versions of the device completely.

Network Topology

Figure 25 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: Configure the IP addresses of the interfaces so that the network between Device and the FTP server is normal. (Omitted)

Step 4: 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
```

#Use the sysupdate command to upgrade the image program of the control card.

```
Device#sysupdate image mpu 2.0.0.1 sp35-g-9.7.20.1(R).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 5: Upgrade the bootloader program.

#Use the sysupdate command to upgrade the bootloader program of the control

card.

```
Device# sysupdate bootloader mpu 2.0.0.1 sz03-tboots2-b6b7-9.6.2.5.pck 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 6: Upgrade the devinfo program.

#Use the sysupdate to upgrade the devinfo program of the control card.

```
Device# sysupdate devinfo mpu 2.0.0.1 devInfo_sw_SOFINET_V2.125 ftp admin admin
```

For the upgrade process of DEVINFO program and the printing information of whether the upgrade is successful, refer to the relevant content of "Devinfo upgrade" in "Software upgrade function configuration".

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)?y
Please confirm system to reload(Yes|No)?y
```

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

Step 7: 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 of the active and standby control cards have been upgraded successfully.

```
Device#show  system  mpu
System Card Information(Mpu 0 - ONLINE)
 ------------------------------------------------------------
```

```
                Type:  SOFOS SFN3300
              Status:  Start Ok
          Last-Alarm:  Normal
       Card-Port-Num:  30
    Card-SubSlot-Num:  0
   Power-INTF-Status:  Normal
   Power-Card-Status:  On
        Serial No.:
       Description:
  Hardware-Information:
              PCB-Version: 001
  Software-Information:
         Bootloader-Version: 9.6.2.5
          Software-Version: 9.7.20.1(integrity)
Temperature-Information:
         Temperature-State:
                  Switch-Temperature = 71 C
                  Last-Alarm = Normal.
                  Mainboard-Temperature = 40 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:  10%
MEM-On-Card-Information:  <1 MEMs>
                MEM-Idx:  00
               MEM-State:
                  BytesFree =  524738560 bytes
                  BytesAlloc =  435757056 bytes
                  BlocksFree =  5 blocks
                 BlocksAlloc =  12380 blocks
               MaxBlockSizeFree =  23068672 bytes
                  SizeTotal =  960495616 bytes
DISK-On-Card-Information:  <1 DISKs>
                DISK-Idx:  00
                  Type:  Flash
                 Status:  Online
               DISK-State:
                  SizeTotal =  162299904 bytes
                  SizeFree =  50569216 bytes
-------------------------------------------------------------
```

```
STATISTICS:        1 IN, 0 OUT, 0 IERR, 0 OERR
Device#show devInfo
vendor        : SOFINET
product Type   : SWITCH
devInfo version: V2.125
```

Note

- The reachable interface between the device and the FTP server can be the dc0 out-of-band management interface or the service interface.
- It does not matter whether the bootloader 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 of the active/standby main control card 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 flash space of the active/standby main control card is recommended to be larger than 170M before the upgrade. Otherwise, the upgrade time may become longer.
- If some programs in the newly released version have not changed, the unchanged programs cannot be upgraded.
- In the process of upgrading, if some boards fail to upgrade due to abnormal conditions, they can be upgraded separately.

2.10.3.3 Upgrade the bootloader Program via the Console Port

Network Requirements

- PC and the Console port of the device are directly connected.
- The bootloader program of the active and standby control cards is to be

upgraded through the Console port.

Network Topology

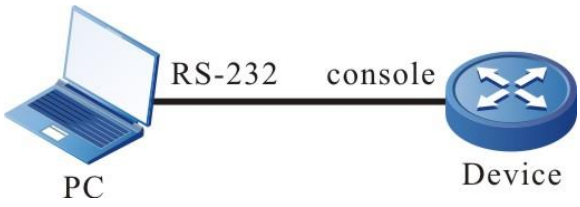


Figure 26 Upgrading the bootloader Program via the Console Port

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 " Press ctrl+c to enter bootloader mode: 0 " 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.

```
Bootloader#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.

```
Bootloader#mupdate bootloader
```

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

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:

```
9.6.2.5 compiled at Mar 03 2020 - 01:15:27
```

```
warm boot from master sector
Press ctrl+c to enter bootloader mode:  0
```

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.

2.11Bootloader

2.11.1 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 the image program, and select the loading mode of the Image program.
- Upgrades the Bootloader program.

- Backs up the bootloader program.

2.11.2 Bootloader Function Configuration

Table 114 Bootloader function configuration list

Configuration Tasks	
Enter the bootloader configuration mode	Enter the bootloader configuration mode when starting
Set the Bootloader boot parameters	Set the Bootloader boot parameters
Configure the IP address of the bootloader management Ethernet port	Configure the IP address of the bootloader management Ethernet port
Upgrade the Bootloader program	Upgrade the Bootloader program

2.11.2.1 Preparation before Configuring the Bootloader Functions

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

2.11.2.2 Enter bootloader Configuration Mode

Configuration Condition

None

Enter bootloader Configuration Mode

Table 115 Enter the bootloader configuration mode

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-b7# #" is prompted.

Note

- After entering the bootloader configuration mode, you can execute the functions provided by the bootloader mode.

2.11.2.3 Set the Bootloader Boot Parameters

Configuration Condition

None

Set bootloader Boot Parameters

Table 116 Set the Bootloader boot 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-b7# #" is prompted.
Set the boot parameters of IOS in bootloader	change *index[0~3]* ge0-3 *filename local-ip-addr host-ip-*	Mandatory The command of the first line is

Step	Command	Description
	addr [gatewayip] [netmask] change *index[0~3]* flash0 *filename*	the network boot configuration parameter. If it is upgrading across the segment, it is necessary to add the gateway and mask. The command of the second line is the boot configuration parameter of the flash storage device.

Note

- Currently, the bootloader program of the switch can set the boot parameter to start the image program via the network.

2.11.2.4 Upgrade the Bootloader Program

Configuration Condition

None

Upgrade the Bootloader Program

Table 117 Upgrade 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-b7# #" is prompted.
Start the tftp service on the PC		Mandatory Copy the new bootloader version

Step	Command	Description
		used for upgrading to the root directory of tftp, used by the device to download the version file via tftp.
Upgrade the Bootloader program	update bootloader*filename* ge0-3 *local-ip-addr host-ip-addr [gatewayip] [netmask]*	Mandatory
Back up the bootloader program	bootloaderbak	Optional

Note

- Bootloader system program adopts dual-bootloader backup mode, which is divided into the master bootloader program and standby bootloader program. With the upgrade command, you can only upgrade the version of the master bootloader, while the standby bootloader program will remain unchanged.
- After upgrading the Bootloader system program, use the command reset or power off to restart the device, and then, you can use the latest Bootloader system program.
- After the system is loaded successfully, you can use the **sysupdate** command to upgrade.

2.11.2.5 Bootloader Monitoring and Maintaining

Table 118 bootloader monitoring and maintaining

Command	Description
version	Display the version number of the bootloader program
print *index[0~4]*	Display the information of the boot parameter specified by index
boot index[0~4]	Load the boot parameter information specified by index
clear index[0~4]	Clear the boot parameter information specified by index

Command	Description
grate	Get the rate of the current serial port
Srate ratenum	Get the rate of the current serial port, 9600 or 115200

2.11.3 Typical Configuration Example of Bootloader

2.11.3.1 Configure bootloader to Start the Image Program via the Network

Network Requirements

- The PC acts as the TFTP server, Device acts as the TFTP client, and the server and device are connected via the network.
- On the TFTP server, place the image program and bootloader program to be upgraded in the TFTP server directory.

Network Topology

Figure 27 Networking for configuring bootloader to start the image program via the network

Configuration Steps

Step 1: Configure the TFTP server, and place the image program in the directory of the TFTP server. (omitted)

Step 2: After the device is powered on, press “Ctrl + C” to enter the bootloader configuration mode.

Step 3: Configure the boot parameters to start the image program from the network.

```
bootloader-b7# # change 0 ge0 sp35-g-9.7.20.1(R).pck 1.1.1.2 1.1.1.1
bootloader-b7# # boot 0
```

Note

- Connect the first port of the device to the tftp server.
- After setting the above boot information, the device can communicate with the tftp server normally before executing boot.

2.12 PoE Management

2.12.1 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.

2.12.1.1 PSE/PD Interface Specifications

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 (1, 2, 3, 6 signal wire pairs) and Alternative B (idle 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.

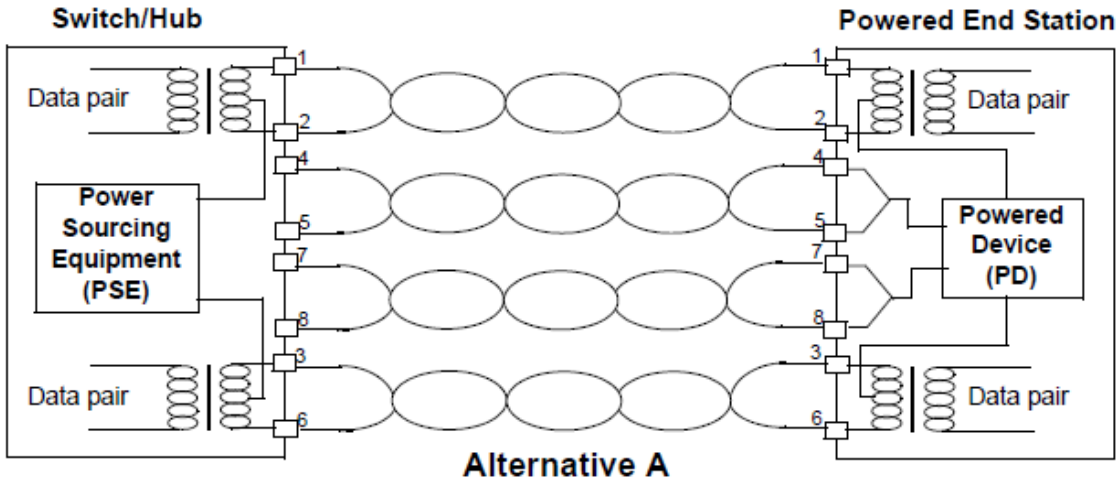


Figure 28 Alternative A Power Supply Mode with 10BASE-T and 100BASE-TX

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.

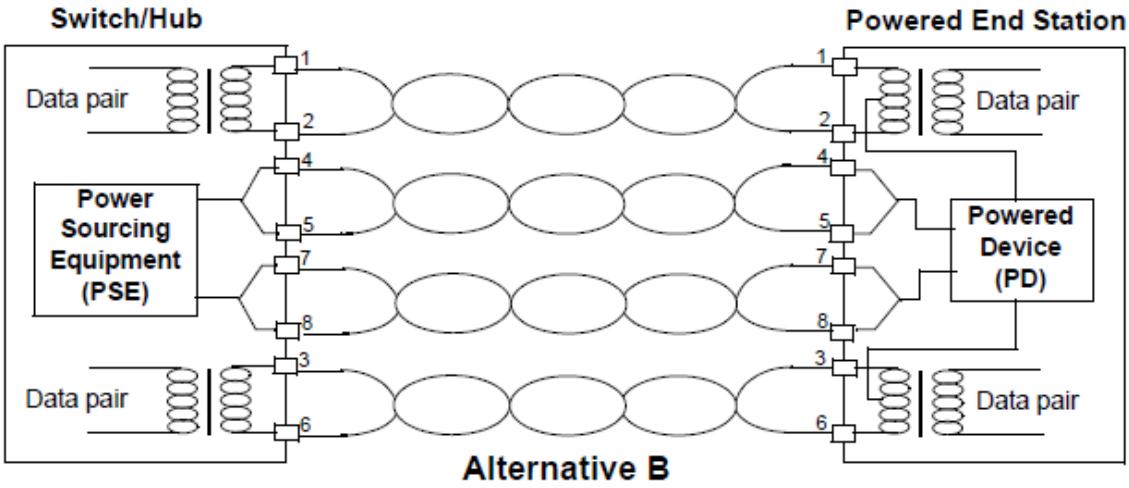


Figure 29 Alternative B Power Supply Mode with 10BASE-T and 100BASE-TX

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.

2.12.1.2 PoE Power Supply Process

If a PSE is installed in a network, the PoE Ethernet power supply process is as follows:

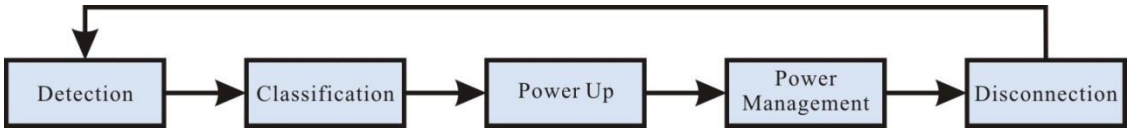


Figure 30 PSE Power Supply Process

- 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.

2.12.2 PoE Function Configuration

Table 119 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.
	Enable the auto power supply function of the 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.
	Configure the maximum output power of an interface.
Configure power supply priorities.	Configure a PoE power management mode.

Configuration Tasks	
	Configure the power supply priority of an interface.
Configure PD power-on and power-off 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 power supply wire pair of the interface
	Configure the power-off detection mode of the interface
Configure the abnormality recovery function.	Configure the time for recovery from a power supply abnormality of an interface.
	Restart the PoE power supply.
Configure the POE power alarm function	Configure the PoE power alarm threshold

2.12.2.1 PoE Basic Function Configuration

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 interface. 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 Condition

None

Enable the Global PoE Function

Table 120 Enabling the Global 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

Step	Command	Description
		enabled.

Enable the Interface PoE Function

Table 121 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 122 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 L2 Ethernet interface configuration mode.	interface *interface-name*	-
Enable the forced power supply function of an interface.	power force	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.

Note

- The auto power supply function of the interface can take effect only in the manual power management mode.

2.12.2.2 Configure PoE Power

Configuration Condition

Before configuring the PoE power, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure 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 123 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 { all | *system-id* { all | *subsystem-id* } } *power-value*	Optional. By default, the total power is the maximum total power that the device power supply can

Step	Command	Description
		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 124 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 { all | *system-id* { all | *subsystem-id* } } *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 125 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 threshold-mode {	Optional.

Step	Command	Description
power limit mode of an interface.	classification | user }	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 126 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*	-
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.

2.12.2.3 Configure Power Supply Priorities

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 Condition

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 127 Configuring a PoE Power Management Mode

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure PoE power management mode.	power manage { all | *system-id* { all | *subsystem-id* } } { dynamic-fifs | dynamic-priority }	Optional. The default power management mode is the dynamic First In First Served (FIFS).

Configure 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 128 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 { all | *system-id* { all | *subsystem-id* } } 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.

2.12.2.4 Configure PD Power-On and Power-off Parameters

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 Condition

Before configuring PD power-on parameters, ensure that:

- The global PoE function is enabled.
- The interface PoE function is enabled.

Configure 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 129 Configuring the PD Detection 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 PD detection	power detect-mode {	Optional.

Step	Command	Description
mode of an interface.	compatible | standard }	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 130 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. This type of PDs are classified to class0 by default, and the maximum output power of the interface is 15.4 watt.

Configure 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 131 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.

Configure the Power-off Detection Mode of the Interface

PSE switches can provide different power failure detection modes according to the current type of power supply, DC or AC.

Table 132 Configure the power-off detection mode of the interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the power-off detection mode of the interface	power disconnect{ ac | dc }	Optional By default, the power-off detection mode is DC.

Note

- The PoE function of PSE equipment is integrated into the switch. The interface power-off detection mode on the device is DC by default and only supports the DC mode.

2.12.2.5 Configure Abnormality Recovery Function

When there is a PoE power supply abnormality, the abnormality recovery function is supported, including automatic recovery and manual recovery.

Configuration Condition

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 133 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 minute, indicating recovery immediately.

Restart 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 134 Configuring the Time for Recovery from a Power Supply Abnormality of an Interface

Step	Command	Description
Restart the PoE power supply.	power reload {all | *system-id*}	Mandatory.

Note

- In the process of power restarting, the module will be initialized, and repeated operation of power reload should be avoided, and it will be executed after the power restart is completed.

2.12.2.6 Configure PoE Power Alarm Threshold

Configuration Condition

Before configuring the PoE power, first complete the following task:

- Enable global PoE function
- Enable interface PoE function

Configure PoE Power Alarm Threshold

When the PoE power utilization reaches or is lower than the set power threshold, send the Trap alarm prompt.

Table 135 Configure the PoE power alarm threshold

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the PoE power alarm threshold	power alarm-threshold { all | *system-id* { all | *subsystem-id* }	Optional By default, the power alarm

Step	Command	Description
	} *threshold-value*	threshold is 99%.

2.12.2.7 PoE Monitoring and Maintaining

Table 136 PoE Monitoring and Maintaining

Command	Description
show power { manage | summary | configure interface *interface-name* | detect interface *interface-name* | pd-status interface *interface-name* | system-to-port [*system-id*] | version }	Display the PoE configuration, the power supply status information, and the power corresponding relation information. There is system-to-port only in the VST mode.

2.13PDI

2.13.1 Overview

PDI: PD device inspection, which refers to a way specially provided for PoE to detect whether the PD terminal is online. If it detects that the PD is not online, it will be considered abnormal and notify Poe to restart the power supply.

PDI function needs to be controlled by configuring interface PDI enable, that is to say, PDI function must be enabled under interface before PDI function can be used.

2.13.2 Configure PDI Basic Functions

Table 137 Enable the interface PDI function

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Enable the interface PDI function	pdi enable	Mandatory By default, the PDI function of the interface is not enabled.

2.13.3 Configure the Interval of Sending ARP Packets

Table 138 Configure the interval of the interface sending the ARP packets

Step	Command	Description
Enter the L2/L3 Ethernet interface	interface *interface-name*	-

Step	Command	Description
configuration mode		
Configure the interval of the interface sending the ARP packets	pdi inspection-interval	Optional By default, the interval of the interface sending the ARP packets is 3s.

2.13.4 Configure Times of Re-transmitting ARP Packets

Table 139 Configure the times of re-transmitting the arp packets

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the times of re-transmitting the arp packets	pdi inspection-retry	Optional By default, the times of the interface re-transmitting the ARP packets is 3.

2.13.5 Configure IP Detection Entry

Table 140 Configure the IP detection entry

Step	Command	Description
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the ip detection entry of PD	pdi ip-address	Optional

2.13.6 PDI Monitoring and Maintaining

Table 141 PDI monitoring and maintaining

Command	Description
show pdi { | brief | interface *interface-name* | ip-entry interface *interface-name* | statistic interface *interface-name* }	Display PDI global structure, port brief information, detailed information, etc

2.14 LUM

2.14.1 Overview

LUM (Local User Manager): The local user database used to provide the AAA local authentication.

RBAC (Role Based Access Control): By establishing the association of "Authority <-> Role", assign the authority to the role, and by establishing the association of "Role <-> User", specify the role for the user, so that the user can get the authority of the corresponding role. The basic idea of RBAC is to specify roles for users. These roles define which system functions and resource objects the users are allowed to operate.

Because of the separation of the authority and the user, RBAC has the following advantages:

- The administrator does not need to specify authorities one by one for users, they just need to define the roles with corresponding authorities in advance, and then assign the roles to users. Therefore, RBAC can better adapt to the changes of users and improve the flexibility of user authority allocation.
- Because the relationship between roles and users often changes, but the relationship between roles and authorities is relatively stable, so using this stable association can reduce the complexity of user authorization management and management cost.

Role: The set of rules

Rule: The permit/deny authority of the commands of the specified features or all features

Feature: Module

2.14.2 LUM Function Configuration

Table 142 LUM function configuration list

Configuration Task	
Configure the user role	Configure the user role
Configure the administrator scheme	Configure the administrator
	Configure the administrator user group
Configure the access user scheme	Configure the access user
	Configure the user group

2.14.2.1 Configure the Role

By default, there are four roles: Security-admin, Network-admin, Audit-admin and Network-operator. The authorities of these four roles cannot be changed.

Customize role authorities as a subset of network administrator role authorities. It is not allowed to configure module authorities that have been granted security-admin and auditor-admin roles. For detailed authorities, refer to the following table:

Table 143 The corresponding authorities of the roles

	Log	History	User management, user authentication	Other Modules
Public	NO	NO	Modify own password	Show running, exit and so on
Security-admin	Operation log query and related configuration commands	History configuration and operation	OK	Lai module, line , service, AAA
Audit-admin	Data log query and configuration commands	NO	NO	NO
Network-admin	All other commands except for the operation log and data log	History configuration and operation	NO	OK
Network-operator	All show commands in the network administrator authority	Show command	NO	All show commands in the network administrator authority

By default, the user does not configure the role attribute. When the role attribute takes effect, the user level does not take effect any more, and the role replaces the user level as the basic criterion of instruction authorization: users have the execution authorities of different instructions according to their roles.

Configuration Conditions

None

Configure User Roles

Table 144 Configure the user role

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one user role and enter the user role mode	role role-name	Mandatory By default, there are four roles: Security-admin, Network-admin, Audit-admin and Network-operator. The authorities of these four roles cannot be changed.
Create a rule for the user role	rule number {deny | permit} feature {all | feature-name }	By default, do not define a rule for the new user role, that is, the current user role has no authorities. The rule modification does not take effect for the current online user, but takes effect for the future user that logs in and uses the rule of the role. The smaller the rule ID, the higher the rule priority.

2.14.2.2 Configure the Local User

Local users are the users stored in devices: including local administrators and local access users. Only when the authentication method is local will it take effect. When you create a local user, you specify whether it is an administrator or an access user.

Configuration Conditions

None

Configure Local Administrator User

Table 145 Configure the administrator

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an administrator user and enter the administrator user mode	local-user user-name class manager	Mandatory By default, do not configure the administrator user.

Configure Local Access User

Table 146 Configure the access user

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an access user and enter the access user mode	local-user *user-name class* network	Mandatory By default, do not configure the access user.

2.14.2.3 Configure Administrator User Attribute

The administrator indicates the user logging into the device.

When configuring the attribute of the local administrator user, there are the following configuration restrictions and instructions:

- If the user authorizes the role through AAA at the time of login, whether the user can execute the command after logging to the device depends on the role. If not authorizing the role through AAA at the time of login, whether the user can execute the command after logging into the device depends on the user level.
- For SSH users, when using public key authentication, when the authentication mode of logging into the device is not configured in the user line view, the commands they can use are based on the user role or user level set in the local administrator user view with the same name as the SSH user (the priority of the user role is higher than the user level). For the detailed introduction to user roles, refer to “Configuration Roles” in “LUM Configuration Guide”.
- The maximum try times of the user password can be configured in the local administrator user view and administrator user group view. The priority order of the configuration in each view is: local administrator user view - > administrator user group view.
- The password lifecycle of the user can be configured in the local administrator user view, the administrator user group view and the global view. The priority order of the configuration in each view is: local administrator user view - > administrator user group view - > global view.

Configuration Conditions

None

Configure the Attribute of Administrator User

Table 147 Configure the attribute of the administrator user

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an administrator user and enter the administrator user mode	local-user *user-name class* manager	Mandatory By default, do not create the administrator user.
Configure the administrator user password	password 0 *password*	Mandatory By default, the user does not have password.
Set the server type that the user can adopt	service-type { ssh | telnet | console | ftp | web}	Mandatory By default, the user does not support any service-type.
Set the user role of the local user	user-role role-*name*	Optional By default, do not configure the administrator role. The priority of the administrator role is higher than the administrator level, that is, when the administrator user is configured with the role, the administrator authority is based on the administrator role.
Set the user group of the administrator user	group *group-name*	Optional By default, do not configure the user group.
Configure the level of the login user authorization	privilege *privilege-level-number*	Optional By default, the default level is 1.
Configure the command that the user automatically executes	autocommand *command-line*	Optional By default, do not configure the command that the user automatically executes.

Step	Command	Description
Configure the option that the user automatically executes the command	autocommand-option { nohangup [delay *delay-time-number*] |delay *delay-time-number* [nohangup] }	Optional By default, disconnect after executing the command automatically and the delay time of automatically executing the command is 0.
Configure the life period of the user	password-control livetime *user-live-time*	Optional By default, do not limit the life period of the user.
Configure the maximum times of the successive login authentication failure of the administrator user	password-control max-try-time max-try-time-number	Optional By default, the user management does not limit the maximum try times.
Configure the maximum online quantity of one user	max-online-num *user-number*	Optional By default, do not limit the maximum online quantity of one user.
Configure the file authority that the user can use	filesys-control{read | write | execute | none}	Optional By default, the user owns the read, write, and execute file authorities.
Configure the directory provided by the device for the administrator to access or manage	work-directory *directory*	Optional By default, it is /flash directory. Currently, the attribute only functions on the file directory of configuring ftp user login device.

2.14.2.4 Configure Access User Attribute

The access user is the user that is connected to the network via the device.

Configuration Conditions

None

Configure the Access User

Table 148 Configure the access user

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one access user and enter the access user mode	local-user *user-name class* network	Mandatory By default, do not configure the access user.
Configure the access user password	password 0 *password*	Mandatory By default, the user does not have password, and as a result, maybe the user cannot log into the device.
Set the server type that the access user can use	service-type { xauth }	Mandatory By default, the user does not support any service-type.
Set the user group of the access user	group *group-name*	Optional By default, do not configure the user group of the access user.
Configure the user status	stat {active / block }	Optional By default, the status of the user is active.

2.14.2.5 Configure the Local User Group

Local users are divided to administrator user group and access user group.

Administrator user group is a set of administrator user attributes, which supports configuring password lifetime and the maximum number of successive login authentication failures.

Access user group is the management of access users, with hierarchical nesting,

which more vividly reflects the organizational structure of the company or department. The access user group does not support any access user attributes.

Configuration Conditions

None

Configure Administrator User Group

Table 149 Configure the administrator user group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an administrator user group and enter its mode	manager-group *group-name*	Mandatory By default, do not configure the administrator user group.
Configure the lifetime of the user password in the administrator user group	password-control livetime *user-live-time*	Optional By default, do not limit the lifetime of the administrator user in the user group, that is, give priority to the password lifetime configured in the administrator user view.
Configure the maximum times of the user successive login authentication failure in the administrator user group	password-control max-try-time max-try-time-number	Optional By default, do not limit the times of the user successive login authentication failure in the administrator user group, that is, give priority to the maximum times of the successive login authentication failure configured in the administrator user view.

Configure Access User Group

Table 150 Configure the access user group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an access user group and enter its mode	user-group group-name	Mandatory By default, do not configure the access user group.
Configure the parent group of the access user group	parent group-name	Optional By default, the default parent group is the parent path in the group name path.

2.14.2.6 Configure the Password Policy

For our system, there is a strong password security policy. Ensure the password security from the complexity of the password, force to modify the password for the initial login, and maximum try times of the password. Password security policy is only valid for local administrator users.

Password complexity:

1. The minimum password length limit allows administrators to limit the minimum password length for administrators. When setting a user password, the system will not allow the password to be set if the length of the password entered is smaller than the set minimum length. And prompt: " Bad password: It must contain at least 2 character(s)."
2. Password combination detection function: The administrator can set the combination type of user password components. The elements of a password include the following four types:

- Capital letters: A-Z
- Lowercase letters: a-z
- Decimal digits: 0-9

- 31 Special Characters: (`~!@$%^&*()_+-={}[]|\:;”’<>,./’)

There are four combination types of password elements, which have the following specific meanings:

- Combination type 1 indicates that there is at least one element in the password.
- Combination type 2 means that there are at least two elements in the password.
- Combination type 3 means that there are at least three elements in a password.
- Combination type 4 means that all four elements must be included in the password.

When the user sets the password, the system will check whether the password set meets the configuration requirements. Only the password that meets the requirements can be set successfully.

1. The password cannot be the same as the user name. When setting the administrator user password, if the password entered is the same as the user name, the system will not allow the password to be set.

Force to modify password for initial login:

When the function of "Force to modify the password when the user logs in for the first time" is enabled, when user first logs into the device, the system will output corresponding prompt information to ask the user to modify the password. Otherwise, the user is not allowed to log into the device. When the administrator's user name is "admin", whether or not the function of "Force to modify the password when the user logs in for the first time" is enabled, the user will be forced to modify the password when logging into the device for the first time.

Password lifetime:

Password lifetime is used to limit the using time of the user password. When the

password is used longer than the password lifetime, the user needs to change the password. When a user logs in, and if the user enters an expired password, the system will prompt the user that the password has expired, and the password must be reset before local login. If the password entered does not meet the requirements, or if the new passwords entered twice are inconsistent, the system will refuse this login. For the non-interactive mode of login, such as FTP users, after the password lifetime expires, the user can log in only after the administrator modifies the password of FTP users; but if the password expires during the login period, it will not affect the operation of this login, but the next FTP command will trigger offline. In particular, if it is required to change the password for the first login, the password in fact has reached the expiration time, and the login will only require a unified password change once.

Maximum try times of the password:

The maximum try times of the user can be used to prevent malicious users from trying to decrypt the code. When the password try fails more than the maximum try times, the system will blacklist the user in the login-security module, and the user's account will be locked for a period of time.

Configuration Conditions

None

Configure Password Policy

Table 151 Configure the password policy

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the complexity of the password	password-control complexity {min-length *len*| with user-name-check | composition type-number *type-number* }	Optional By default, the minimum length of the user password is 6, the combination type of the password elements contains

Step	Command	Description
		two kinds, and does not permit the user name to be the same as the password.
Configure forcing to modify the password when the user logs in for the first time	password-control firstmodify enable	Optional By default, do not force the user to modify the password when the user logs in for the first time. When the user named “admin” does not enable the command, it is also required to modify the password when logging in for the first time.
Configure the live time of the user	password-control livetime *user-live-time*	Optional By default, do not limit the live time of the user.
Configure the maximum times of the successive login authentication failure of the administrator user	password-control max-try-time max-try-time-number	Optional The command is configured in the administrator user group and administrator user. By default, the successive login authentication failure of the user in the administrator user group is not configured, that is, take the maximum times of the successive login authentication failure configured in the administrator user view as the main.

2.14.2.7 LUM Monitoring and Maintaining

Table 152 LUM monitoring and maintaining

Command	Description
debug user { manager | network}	Enable the debug information of the user management
show users class { manager | network } [*username*]	Display the configuration information of the user
show role [*rolename*]	Display the configuration information of all roles or specified role

2.14.3 LUM Typical Configuration Example

2.14.3.1 Configure Network Administrator User

Network Requirement

- Configure the network administrator user, and verify whether it has the network administrator authority.

Network Topology

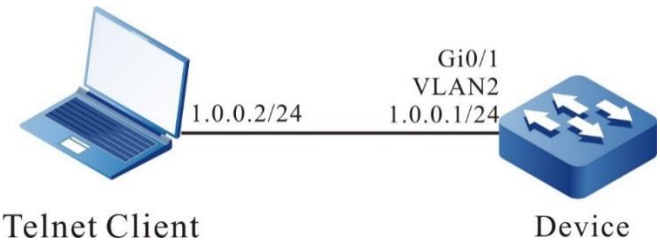


Figure 31 Networking for configuring the network administrator user group

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Configure the administrator attributes.

#Configure the user as admin and password as admin.

```
Device#configure terminal
Device(config)#local-user admin class manager
Device(config-user-manager-admin)#password 0 admin
```

#Configure the service type.

```
Device(config-user-manager-admin)#service-type telnet ftp web console ssh
```

#Configure the role of the local user as the network administrator.

```
Device(config-user-manager-admin)#user-role network-admin
```

#Configure the local authorization, making the role take effect.

```
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 using the login aaa authentication in line vty.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
```

Step 3: At the Telnet client, input the user name admin and password admin, and log into the device successfully.

#View whether the administrator user can execute the administrator command **show logging** to view the logs.

```
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:
```

#Verify that the network administrator cannot execute the commands of other administrators.

```
Device#show role
You may not be authorized to perform this operation,please check.
```

Note

- The default roles of the administrator have security-admin, network-operator, audit-admin, and network-admin. You can set the administrator role according to the demand, and also can the customized role.

2.15 ZTP

2.15.1 Overview

ZTP (zero touch provisioning) refers to the function of automatically loading version files (including system software, configuration files, license files, patch files, and customized files) when the new factory or empty configuration device is powered on and started.

The purpose is to solve the problem that when the network equipment is deployed, the administrator needs to go to the installation site to debug the software of the equipment after the hardware installation of the equipment is completed. When the number of devices is large and the distribution is wide, administrators need to manually configure each device, which not only affects the efficiency of deployment, but also requires high labor costs. With ZTP function, the device can obtain the version file from U disk or file server and load it automatically, so as to realize the device free of on-site configuration and deployment, so as to reduce the labor cost and improve the deployment efficiency.

ZTP is not a standard protocol, but a zero-configuration solution of equipment proposed by various manufacturers according to the market demand. There are differences in the implementation details, but the basic process is consistent. ZTP has many ways to start. SOFINET currently supports DHCP zero-configuration starting, USB zero-configuration starting, and email starting. The process is that after the device enables the ZTP function, the empty configuration starting automatically enters the ZTP process. First, try to complete the auto opening through the inserted U disk. If the U-disk opening fails, try to complete the auto opening through DHCP.

The typical networking of DHCP zero-configuration starting is shown in Figure 14-1. When the null-configuration device enters the DHCP zero-configuration starting process, it will first broadcast the DHCP discovery packet through the DHCP client. If the DHCP server and the zero-configuration starting device are not in the same network

segment, it needs to configure the DHCP relay to send the DHCP discovery message across network segments. When the DHCP server receives the DHCP discovery packet, it will assign the temporary IP address, default gateway and other information. At the same time, the intermediate file server address is returned. Then the DHCP client receives the response packet from the DHCP server, parses the address of the intermediate file server and other information, and downloads the intermediate file through FTP/TFTP/SFTP. SOFINET currently supports the intermediate file of the XML format. Finally, analyze the intermediate file, download and upgrade the corresponding version and configuration from the intermediate file server according to the SN (serial number) of the device, and restart the device to take effect.

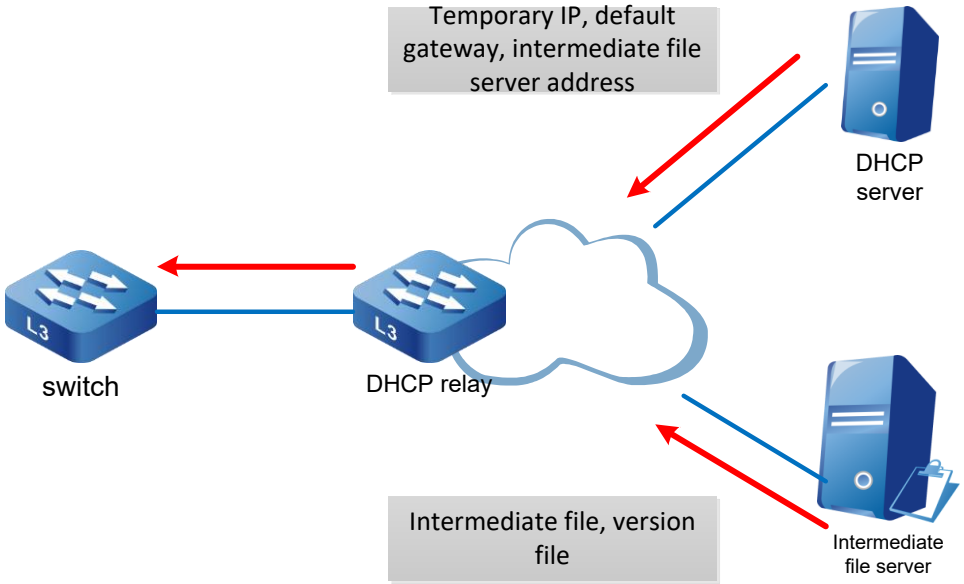


Figure 32DHCP typical networking

DHCP server: It is used to assign temporary management IP address, default gateway, intermediate file server address and other information to the device executing ZTP.

DHCP relay: when the device executing ZTP and the DHCP server are located in different network segments, it is necessary to forward the DHCP interactive packet through the DHCP relay.

Intermediate file server: It is used to save the intermediate files (the type of intermediate file is XML format), version files and configuration files needed by the

device in ZTP process. The device executing ZTP can obtain the file server address, the corresponding version file and configuration file storage path and other information by parsing the intermediate file. The intermediate file server supports TFTP, FTP and SFTP.

Version file server: used to save the version files needed by the device, such as system software and configuration files. Version file server and intermediate file server can be deployed on the same file server, and support three types of TFTP, FTP and SFTP.

USB zero-configuration starting process: users edit the intermediate file, system version, configuration file and other information in advance and save them to USB, and then insert USB into the device to be zero-configuration started. When the device is powered on and detects the USB with the intermediate file meeting the conditions, it will enter the USB zero-configuration starting process, traverse the intermediate file according to the SN of the device, copy the corresponding system version and configuration file from USB, and then restart the device to take effect.

2.15.2 ZTP Function Configuration

2.15.2.1 Enable or Disable ZTP Function

Table 153 Enable or disable the ZTP function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the ZTP function	ztp enable	By default, the device does not enable the ZTP function.
Disable the ZTP function	no ztp enable	-

2.15.2.2 ZTP Monitoring and Maintaining

Table 154 ZTP monitoring and maintaining

Command	Description
show ztp	Display the ZTP information
[no] debug ztp	Enable or disable the ZTP debugging

2.15.3 ZTP Typical Configuration Example

2.15.3.1 Configure ZTP to Use Common Intermediate Files for Zero-configuration Deployment via DHCP

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- As a DHCP server, Device2 provides the DHCP service for ZTP startup process.
- As a file server, Server1 provides FTP services (or TFTP, SFTP services) required by ZTP startup process.
- As a log server, Server2 receives the log information generated during ZTP startup.

Network Topology

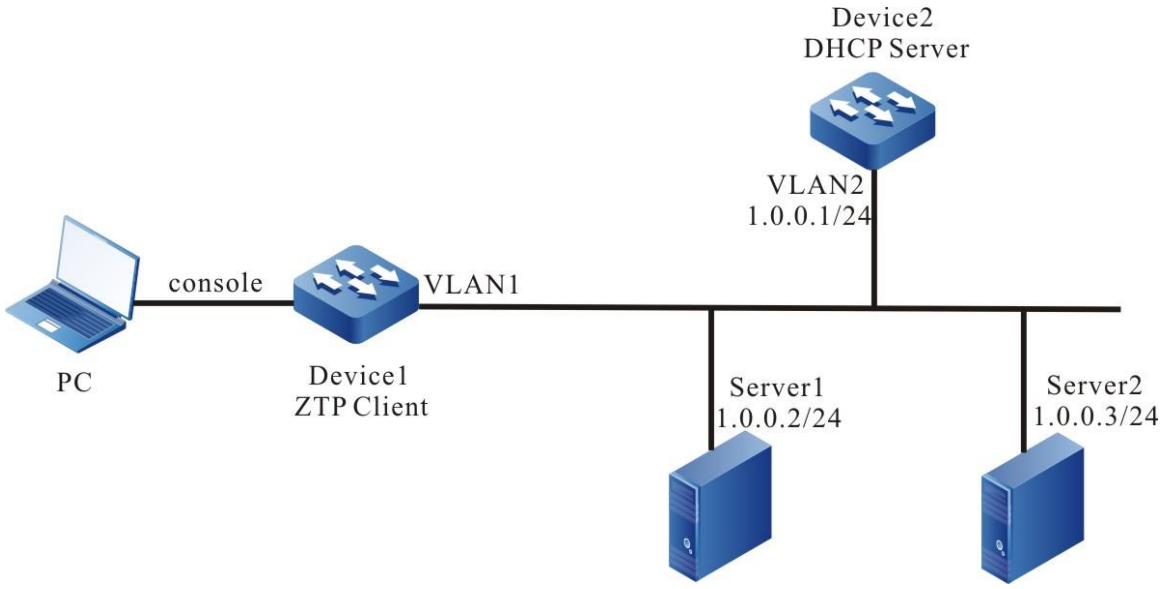


Figure 33 Networking for configuring the device to use the common intermediate file for zero-configuration deployment via DHCP

Configuration Steps

Step 1: To configure the FTP server, you will need to place the version files of the intermediate files (such as ztp.xml) and device configuration file to be downloaded in the directory of FTP server. (omitted)

#The method of editing ordinary intermediate files is as follows:

Right click to open editing in Excel mode

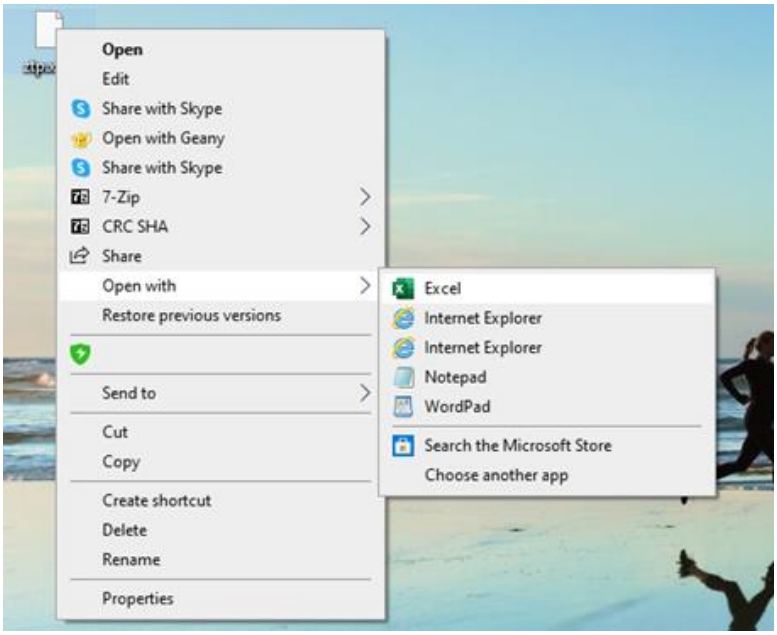


Figure 34 Open XML file graph with Excel to edit

Select as the XML table, and click OK.

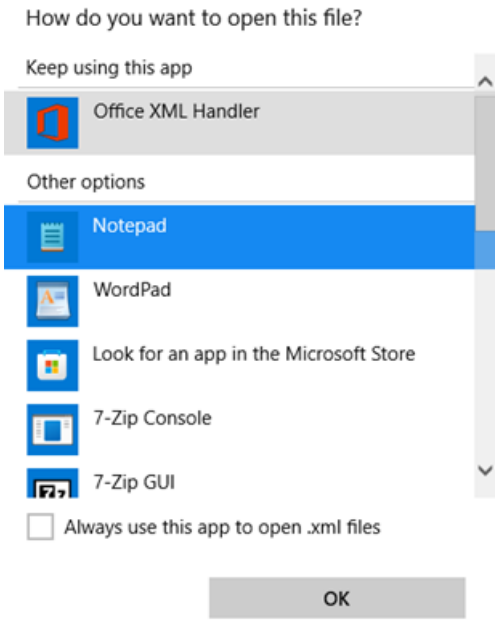


Figure 35 Open as XML table.

You can edit it in Excel. Fill in the device serial number, version file name, version file name, MD5 check value, configuration file name, configuration file MD5 verification sum description information, and finally save it. Note that saving is in XML mode.

	A	B	C	D	E	F
1	Serial-Number	Image-File	Image-File-MD5	Config-File	Config-File-MD5	Description
2	example_1:123456789	xxx.pck	xxx	startup	xxx	
3	example_1:123456789			startup		

Figure 36 Edit the version and configuration file name in the XML file

Step 2: Configure the DHCP service of Device2.

```
Device2#configure terminal
Device2(config)#ip dhcp pool ztp
Device2 (dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure the intermediate file name option.

```
Device2 (dhcp-config)#option 67 ascii ztp.xml
```

#Configure the file download method and server address, user name and password options

```
Device2 (dhcp-config)#option 66 ascii ftp://a:a@1.0.0.2
```

#Configure the log server address option.

```
Device2 (dhcp-config)#option 7 ip 1.0.0.3
Device2 (dhcp-config)#exit
```

#The server enables the DHCP service.

```
Device2(config)#interface vlan2
Device2 (config-if-vlan2)#ip address 1.0.0.1/24
Device2 (config-if-vlan2)#ip dhcp server
Device2 (config-if-vlan2)#end
```

Step 3: Device1 starts with empty configuration, enters ZTP process, downloads version upgrade and loads configuration file.

#Through the following log, you can see that the device enters the ZTP process, and sends the DHCP request.

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, DHCP discovery phase started...
```

#During the ZTP request period, you can exit the ZTP process through Ctrl + C, so that the null configuration can be started. If you do not press Ctrl + C, you can continue to follow the ZTP process.

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successful, and download the common intermediate file.

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Dhcp discovery phase success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to download temp file ztp.xml...
```

#Analyze the intermediate file, and download the version information.

```
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download temp file ztp.xml is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to parse temp file...
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,parse temp file is success
Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to download the Image file ztp.pck
```

#Download the version and configuration file successfully, and then restart the device automatically through ZTP.

```
Apr 22 2020 06:09:26 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download the Image file is success

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Start to download the config file startup_ztp...

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Download the config file is success

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,Dhcp upgrade is success

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,System will rebooted by DHCP upgrade
```

Step 4: Check the result.

Check the ZTP status through show ztp, execute the commands **show running config** and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp
Last ztp method: DHCP upgrade method
  Ztp state: ZTP DHCP upgrade success
  Ztp important inforamtion:
    FTP server IP: 1.0.0.2
    Temporary file name: ztp.xml
    Startup file name:startup_ztp
    Image file name:ztp.pck
Current ztp method: None upgrade method
```

Note

- The device obtains the file download method through option 66 of DHCP protocol, supporting FTP, TFTP and SFTP. You can choose any download method during configuration.
- If the common intermediate file version information is empty, the device ZTP process will not upgrade the version, but only load the configuration

and continue the ZTP process, but the configuration file cannot be empty.

- MD5 of the version file and MD5 of the configuration file are used to check the integrity of the version file and the configuration file.
- If the option 66 is not issued, the TFTP server address can also be directly issued through option 150. At this time, the intermediate file, version file and configuration file can be downloaded through the TFTP server.

2.15.3.2 Configure ZTP to Use python Intermediate Files for Zero-configuration Deployment via DHCP

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- As a DHCP server, Device2 provides the DHCP service for ZTP startup process.
- As a file server, Server1 provides FTP services (or FTP and SFTP services) required by ZTP startup process.
- As a log server, Server2 receives the log information generated during ZTP startup.

Network Topology

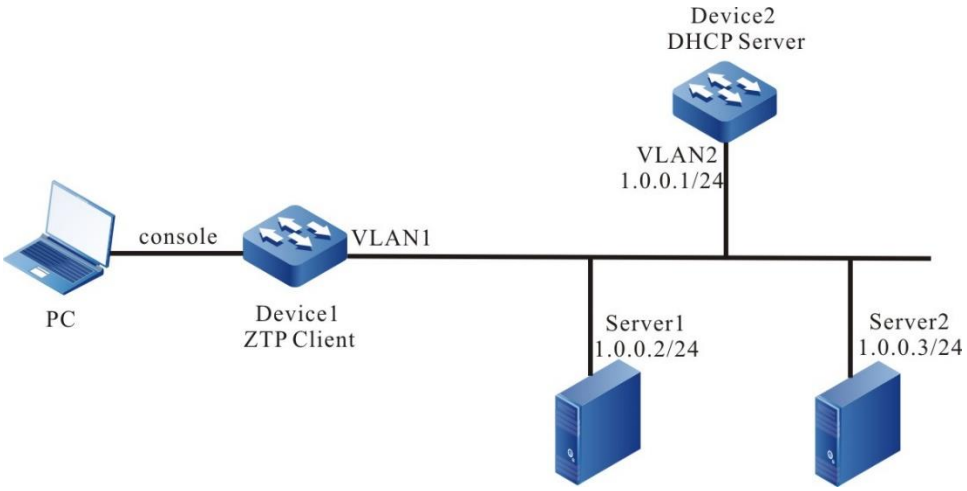


Figure 37 Networking for configuring the device to use the python intermediate file for zero-configuration deployment via DHCP

Configuration Steps

Step 1: To configure the FTP server, you will need to place the version files of the intermediate files (such as ztp.xml) and device configuration file to be downloaded in the directory of FTP server. (omitted)

#Ordinary Python files can be edited with any code editor

#Configure the total file space required by ZTP.

```
required_space = 100
```

#Configure the file downloading mode, and download timeout.

```
protocol = "tftp"
username = ""
password = ""
hostname = "1.0.0.2"
timeout = 1200
```

#The version can be found through the version series, and the version series can be queried through the delivery list.

```
REMOTE_IMAGE_FILE = {
'SOFOS SFN3300 24P4X(V1)' : 'ztp.pck'
}
```

#Configure the remote path to facilitate searching on the server when TFTP downloads files.

```
remote_config_path = "/flash"
remote_pck_path = ""
```

#Configure the checksum MD5.

```
remote_config_is_exist_md5 = False
remote_pck_is_exist_md5 = False
```

Step 2: Configure the DHCP service of Device2.

```
Device2#configure terminal
Device2(config)# ip dhcp pool ztp
Device2 (dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure the intermediate file name option.

```
Device2 (dhcp-config)#option 67 ascii ztp.py
```

#Configure the file download method and server address, user name and password options.

```
Device2 (dhcp-config)#option 66 ascii tftp://1.0.0.2
```

#Configure the log server address option.

```
Device2 (dhcp-config)#option 7 ip 1.0.0.3
Device2 (dhcp-config)#exit
```

#The server enables the DHCP service.

```
Device2(config)#interface vlan2
Device2 (config-if-vlan2)#ip address 1.0.0.1/24
Device2 (config-if-vlan2)#ip dhcp server
Device2 (config-if-vlan2)#end
```

Step 3: Device1 starts with empty configuration, enters ZTP process, downloads version upgrade and loads configuration file.

#Through the following log, you can see that the device enters the ZTP process, and sends the DHCP request.

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, DHCP discovery phase started...
```

#During the ZTP request period, you can exit the ZTP process through Ctrl + C, so that the null configuration can be started. If you do not press ctrl+c, you can continue to follow the ZTP process.

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successfully, and download the common intermediate file.

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Dhcp discovery phase success

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to download temp file ztp.py...

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Download temp file ztp.py is success
```

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789, Start to parse temp file...

#Directly execute the python script.

```
Execute python script start ...

/flash free space is 168(M).

Start to get remote and local file path.

remote config path is /flash/123456789.cfg

Get remote and local file path is success.

remote PCK path is ztp.pck

Start to download image file ztp.pck...

Download image file is success

Start to set boot image file /flash/ztp.pck...
```

#Download the version and configuration file successfully, and then restart the device automatically through ZTP

```
Apr 22 2020 06:09:26 Device1 MPU0 %SYS_UPDATE-RESULT-5:image : Mpu 0 upgrade successfully!

Set boot image file is success.

Start to download config file /flash/123456789.cfg...

Download config file is success.

Start to parse config file /flash/startup...

Parse config file is success.

Execute python script success.


Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,script execute success

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:123456789,System will rebooted by DHCP upgrade
```

Step 4: Check the result.

Check the ZTP status through **show ztp**, execute the commands **show running**

config and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp

Last ztp method: DHCP upgrade method
   Ztp state: ZTP DHCP upgrade success
   Ztp important inforamtion:
      TFTP server IP: 1.0.0.2
      Temporary file name: ztp.py

Current ztp method: None upgrade method

Next ztp state: disable
```

Note

- The device can obtain the file download mode through option66 of the DHCP protocol, and supports FTP, TFTP and SFTP. You can choose any download mode during configuration.
- The server download mode issued by the DHCP server is used to download intermediate files, while the download mode set in Python file is used to download version files and configuration files. There is no inevitable correlation between the two.
- If the version information is not found through the device sequence, the ZTP process of the device will not upgrade the version, but will only load the configuration and continue the ZTP process, but the configuration file cannot be empty.
- If the file download method is TFTP, the user name and password columns must be empty strings, and the two parameters cannot be deleted directly.
- The configuration file name downloaded by the device is composed of serial number and the suffix .md5. For example, if the device serial number

is 12345, then the configuration file name is 12345.md5, and the MD5 verification file is 12345 cfg.md5.

- After downloading the python file, the device will execute the python file directly, so the python file must conform to the python syntax.

2.15.3.3 Configure ZTP to Use Common Intermediate Files for Zero-configuration Deployment via USB

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- Device1 is inserted into the USB device. The USB device contains intermediate file, version file, and device configuration file.

Network Topology

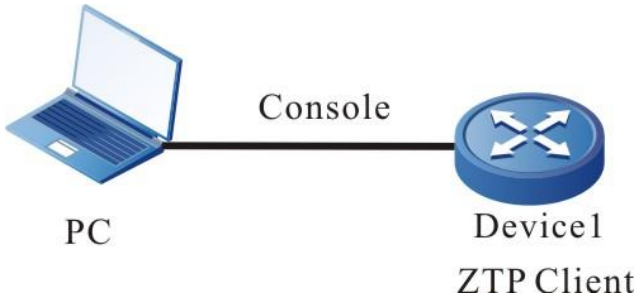


Figure 38 Networking for configuring the device to use the common intermediate file for zero-configuration deployment via DHCP

Configuration Steps

Step 1: Place the intermediate file in the USB root directory, and name as ztp_config.xml, that is /usb/ztp_config.xml.

#The method of editing the common intermediate file is as follows:

Right-click, and open by Excel to edit.

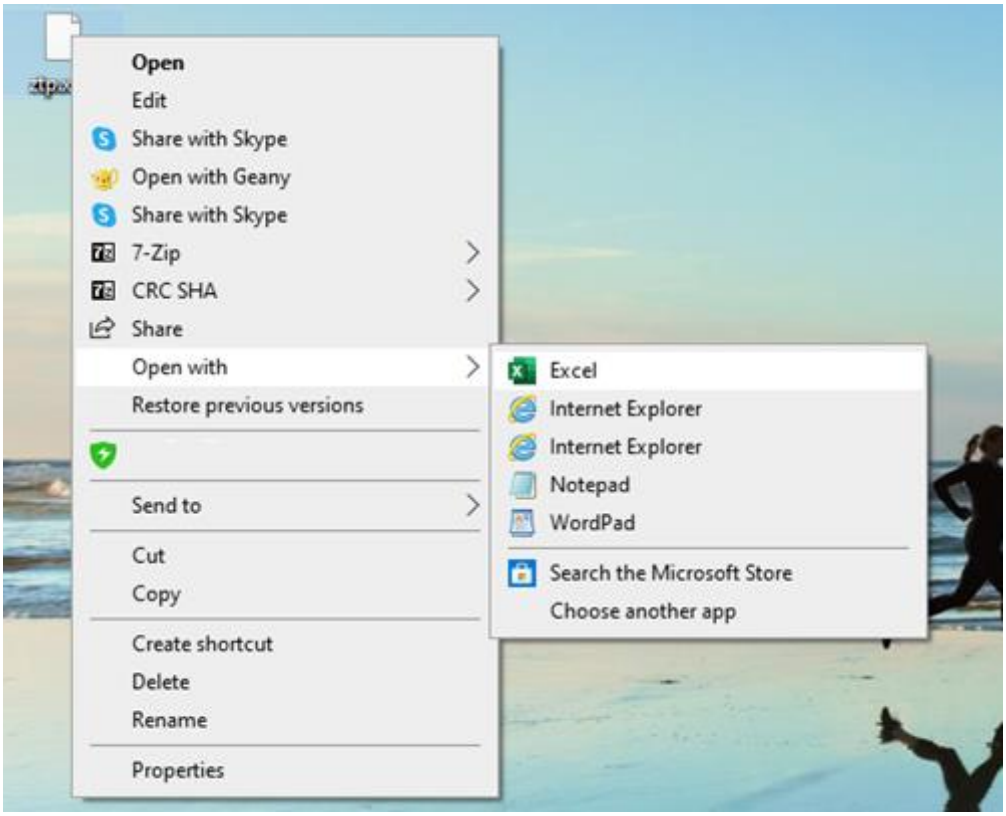


Figure 39 Open XML file graph with Excel to edit

Select as the XML table, and click OK.

You can edit it in Excel. Fill in the device serial number, version file name, version file name, MD5 check value, configuration file name, configuration file MD5 verification sum description information, and finally save it. Note that saving is in XML mode.

	A	B	C	D	E	F
1	Serial-Number	Image-File	Image-File-MD5	Config-File	Config-File-MD5	Description
2	example_1:123456789	xxx.pck	xxx	startup	xxx	
3	example_1:123456789			startup		

Figure 40 Edit the version and configuration file name in the XML file

Note

- XXX is the corresponding IOS version name in USB.
- The XML intermediate file is obtained from the ZTP path of the software release manual.
- In XML intermediate file, the required fields are serial number, version and configuration file, and serial number can be obtained from the equipment delivery list; the version name and configuration file name filled in the XML intermediate file must be consistent with the IOS version file name and configuration file name in USB. Otherwise, the opening fails.
- MD5 code, MD5 code of configuration file, and description information in XML intermediate file are optional. If MD5 code is required, it can be generated by general MD5 code calculation tool.

Step 2: Put the version file and configuration file corresponding to the device serial number in the intermediate file into the USB root directory, and the name is consistent with the description of the intermediate file. (omitted)

Step 3: Power on the device, enter the ztp process, and perform the deployment by USB.

#The device configuration is empty, and enter the USB deployment process.

```
the current config file /flash/startup does not exist.
The backup file /backupramfs/startup is not exist.
The current config file /backup/startup does not exist.
May  6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Now starting USB upgrade...
```

#Search and analyze the intermediate file.

```
May 6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to copy the temporary file /usb/ztp_config.xml...
May  6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Copy the temporary file is success.
May  6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to parse the temporary file /flash/ztp_config.xml
```

#Upgrade the version and configuration.

```
May  6 2020 15:16:15 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Parse temporary file is success

May  6 2020 15:19:53 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Sysupdate image is success

May  6 2020 15:19:53 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Start to copy config...

May  6 2020 15:19:54 Device1 MPU0 %ZTP-USB_UPGRADE-5:SerialNum:123456789,Copy config is success
```

#Restart after upgrading.

```
May  6 2020 15:19:54 Device1 MPU0 %ZTP-USB_UPGRADE-4:SerialNum:123456789,System will be rebooted by USB Upgrade
```

Step 5: Check the result.

#Check the ZTP status via the command **show ztp**. Execute the commands **show running-config** and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp

Last ztp method: USB upgrade method
   Ztp state: ZTP USB Upgrade success
   Ztp important information:
      Temporary file name:/usb/ztp_config.xml
      Startup file name:startup
      Image file name:ztp.pck
Current ztp method: None upgrade method
Next ztp state: disable
```

Note

- If the general intermediate file version information is empty, then the ZTP process of the device will not upgrade the version, but only load the configuration and continue the ZTP process, but the configuration file cannot be empty.
- The device will copy and download the version and configuration file from USB, so it is necessary to put the version and configuration file into USB.
- The name of ordinary intermediate file in USB can only be ZTP_

config.xml.

2.15.3.4 Configure ZTP to Use python Intermediate Files for Zero-configuration Deployment via USB

Network Requirement

- The PC, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- Device1 is inserted into the USB device. The USB device contains intermediate file, version file, and device configuration file.

Network Topology

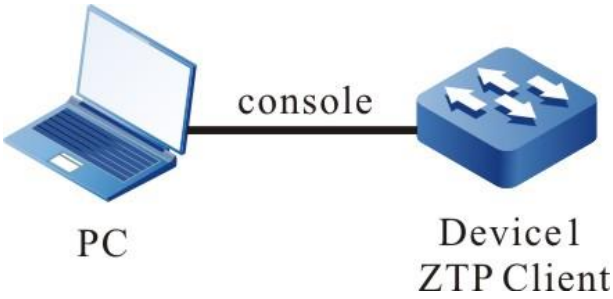


Figure 41 Networking for configuring the device to use the python intermediate file for zero-configuration deployment via USB

Configuration Steps

Step 1: Place the intermediate file in the USB root directory, and name as ztp_script.py, that is, /usb/ztp_script.py.

#Ordinary Python files can be edited with any code editor.

#Configure the total file space required by ZTP, and the unit is MB.

```
required_space = 100
```

#Search for the version through the version series, and the version series can be queried through the delivery list

```
REMOTE_IMAGE_FILE = {'SOFOS S3230' : 'ztp.pck'}
```

#Configure the remote path, and search for the version file and configuration file in the /usb path.

```
remote_config_path = "/usb"
remote_pck_path = "/usb"
```

Step 2: Copy the version file and device configuration file to the USB root directory. The version name is consistent with the version file corresponding to the device serial number. The configuration file name is a file composed of the device serial number and the suffix .cfg. For example, if the device serial number is 12345, the configuration file name is 12345.cfg. (omitted)

Step 3: Insert USB into the device, power on, enter the ZTP process, and start with USB.

#If the configuration file does not exist, USB is inserted into the device to enter the USB start process of ZTP

The current config file /flash/startup does not exist.

The backup file /backupramfs/startup is not exist.

The current config file /backup/startup does not exist.

Apr 30 2020 11:10:12 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,Now starting USB upgrade...

#Search for and analyze the intermediate file.

Apr 30 2020 11:10:12 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,Start to copy the temporary file /usb/ztp_script.py...

Apr 30 2020 11:10:12 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,Copy the temporary file is success.

Apr 30 2020 11:10:12 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,:Start to parse the temporary file /flash/ztp_script.py

#Call python to execute the intermediate file.

Execute python script start ...

#Check the remaining space.

/flash free space is 159(M).

#Download the configuration and version files.

Start to get remote and local file path.

Get remote and local file path is success.

Start to set boot image file /usb/ztp.pck...

```
Apr 30 2020 11:13:51 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,image : Mpu 0 upgrade successfully!Set boot image file is success.

Start to copy config file /usb/12345.cfg...

Copy config file is success.

Start to parse config file /flash/startup...

Parse config file is success.
```

#Download successfully, and restart the effective version and configuration.

```
Execute python script success, reboot device.

Apr 30 2020 11:13:54 Device1 MPU0 %SYS_UPDATE-RESULT-5:SerialNum:123456789,script execute success

Apr 30 2020 11:13:54 Device1 MPU0 %SYS_UPDATE-RESULT-4:SerialNum:123456789,System will be rebooted by USB Upgrade
```

Step 4: Check the result.

#Check the ZTP status via the command **show ztp**. Execute the commands **show running-config** and **show version**, and you can see that the configuration and version take effect.

```
Device1#show ztp

Last ztp method: USB upgrade method
  Ztp state: ZTP USB Upgrade success
  Ztp important information:
    Temporary file name:/usb/ztp_script.py
    Startup file name:startup
    Image file name:ztp.pck

Current ztp method: None upgrade method

Next ztp state: disable
```

Note

- After downloading the python file, the device will execute the python file directly, so the python file must conform to the python syntax.
- The device can obtain the file download mode through option66 of the DHCP protocol, and supports FTP, SFTP and TFTP. You can choose any download mode during configuration.

- If the version information is not found through the device sequence, the ZTP process of the device will not upgrade the version, but will only load the configuration and continue the ZTP process, but the configuration file cannot be empty.
- The configuration file name downloaded by the device is composed of serial number and the suffix .md5. For example, if the device serial number is 12345, then the configuration file name is 12345.md5, and the MD5 verification file is 12345 cfg.md5.
- The device will copy and download the version and configuration file from USB, so it is necessary to put the version and configuration file into USB.
- The name of ordinary intermediate file in USB can only be ztp_ script.py.

2.15.3.5 Configure ZTP to Use python Intermediate Files for Auto Stacking via DHCP

Network Requirement

- The PC1, as the Console control terminal, is used to monitor the ZTP startup process of the device.
- As a DHCP server, Device3 provides the DHCP service for ZTP startup process.
- As a file server, Server1 provides FTP services (or SFTP and TFTP services) required by ZTP startup process.
- As a log server, Server2 receives the log information generated during ZTP startup.
- The stacking of Device1 and Device2 is completed by using T Te0/50 as the stacking link.

Network Topology

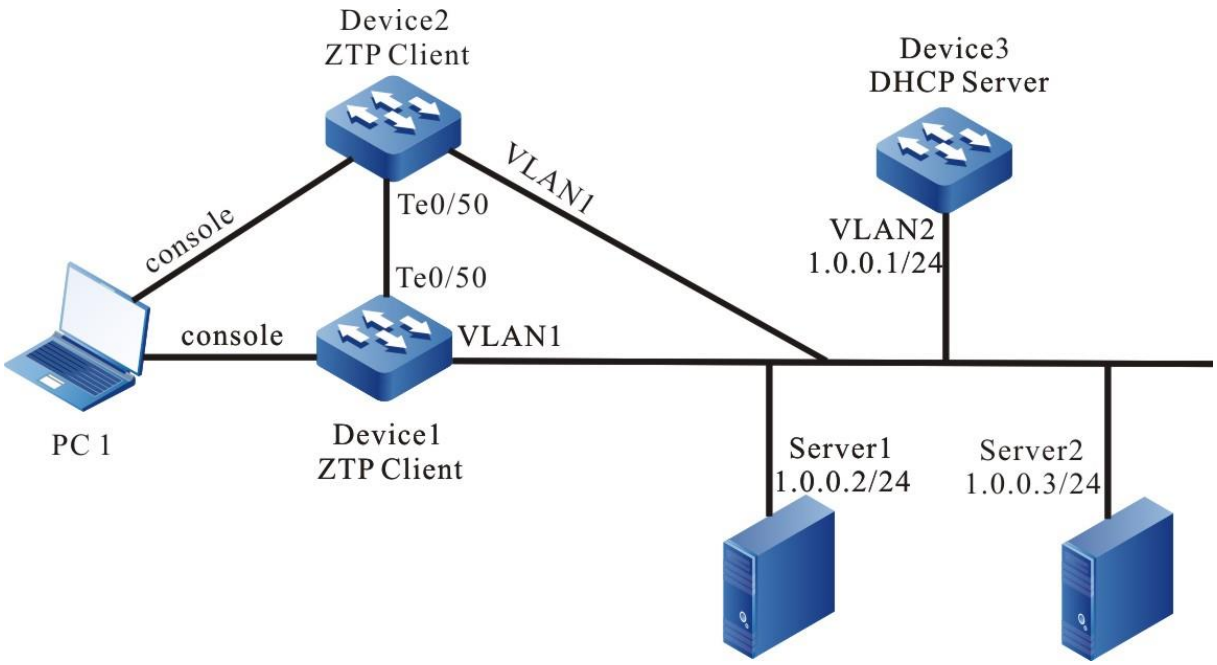


Figure 42 Networking for configuring ZTP to use the python intermediate file for auto stacking via DHCP

Configuration Steps

Step 1: Configure the FTP server, edit the intermediate file, and place the version files of the intermediate files (such as ztp.py) and serial number in the directory of FTP server. (omitted)

#Ordinary Python files can be edited with any code editor.

#Configure the total file space required by ZTP

```
required_space = 100
```

#Configure the file downloading mode and downloading timeout.

```
protocol = "ftp"
username = "a"
password = "a"
hostname = "1.0.0.2"
timeout = 1200
```

#Search for the version via the version series, and the version series can be queried by the delivery list.

```
REMOTE_IMAGE_FILE = {'SOFOS S3230' : 'ztp.pck'}
```

#Configure the remote path so that FTP can find files on the server when downloading files

```
remote_config_path = ""
remote_pck_path = ""
remote_stack_path = ""
```

#Configure the check MD5.

```
remote_config_is_exist_md5 = True
remote_pck_is_exist_md5 = True
remote_stack_is_exist_md5 = True
```

Step 2: Edit the stacking files and configuration files, and upload them to the server for ZTP process downloading.

Here, we assume that the serial number of Device1 is 12345 and that of Device2 is 12340.

#Edit the stacking file.

The stacking file is named by serial number plus .stack. The stacking file name of Device1 is 12345. stack, and the corresponding MD5 check file is 12345 stack.md5 The stacking file name of Device2 is 12340. Stack, and the corresponding MD5 check file is 12340 cfg.md5 。

The stacking file content: contains serial number, stacking domain number, stacking device member

The stacking file content of Device1 is:

```
12345 101  1
```

The stacking file content of Device2 is:

```
12340 101  0
```

#Edit the configuration file. The name of the configuration file is the device serial number plus the suffix .cfg, so the name of the configuration file of Device1 is 12345.cfg, and the corresponding MD5 check file is 12345 cfg.md5 The configuration

file name of Device2 is 12340.cfg, and the corresponding MD5 check file is 12340 cfg.md5.

The stacking part in the configuration file must contain! VST_CONFIG_BEGIN and! VST_CONFIG_END. Slot port configuration must contain! PORT_CONFIG_BEGIN and! PORT_CONFIG_END. The interface dimension set in the configuration file must be a stacking interface dimension, not a stand-alone dimension.

Therefore, the configuration file of Device1 contains

```
!VST_CONFIG_BEGIN
!mode vsl information
vsl-channel 1/1
 exit
!mode vsl end

!slot 0/0
interface tengigabitethernet1/0/50
 vsl-channel 1/1 mode on
 exit
!PORT_CONFIG_END
!VST_CONFIG_END
```

The configuration file of Device2 contains:

```
!VST_CONFIG_BEGIN
!mode vsl information
vsl-channel 0/1
 exit
!mode vsl end

!slot 0/0
interface tengigabitethernet0/0/50
 vsl-channel 0/1 mode on
 exit
!PORT_CONFIG_END
!VST_CONFIG_END
```

After uploading the configuration files and stack files to the server, there are the files: 12345.cfg, 12340.cfg, 12345.cfg.md5, 12340.cfg.md5.

Step 3: Configure the DHCP service of Device3.

```
Device3#configure terminal
Device3(config)# ip dhcp pool ztp
Device3(dhcp-config)#range 1.0.0.4 1.0.0.10 255.255.255.0
```

#Configure the intermediate file name option.

```
Device3(dhcp-config)#option 67 ascii ztp.py
```

#Configure the file downloading method and server address, user name and password.

```
Device3(dhcp-config)#option 66 ascii ftp://a:a@1.0.0.2
```

#Configure the log server address option.

```
Device3(dhcp-config)#option 7 ip 1.0.0.3
Device3(dhcp-config)#exit
```

#The server enables the DHCP service.

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip address 1.0.0.1/24
Device3(config-if-vlan2)#ip dhcp server
Device3(config-if-vlan2)#end
```

Step 4: Device1 and Device2 start with empty configuration, enter ZTP process, download version upgrade and load configuration file.

Device1:

#From the following logs, you can see that the device enters the ATP process and sends the DHCP request.

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Now starting dhcp upgrade...
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, DHCP discovery phase started...
```

#During the ZTP request period, you can exit the ZTP process through ctrl+c, so as to start with empty configuration. If you do not press Ctrl + C, you can continue to follow the ZTP process.

```
Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Press (ctrl + c) to abort Dhcp Upgrade
```

#Get the address successfully, and download the common intermediate file.

```
Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.4, mask 255.255.255.0.

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Dhcp discovery phase success

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Start to download temp file ztp.py...

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Download temp file ztp.py is success

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345, Start to parse temp file...
```

#Directly execute the python script.

```
/flash free space is 100(M).

Start to get remote and local file path.

Get remote and local file path is success.
```

#Download the version.

```
Start to download image file /flash/ztp.pck...

Download image file is success

Start to set boot image file /flash/ztp.pck....

#Download and analyze the stacking file and configuration file.

Start to download stack file /flash/12345.stack...

Download stack file is success.

Start to download config file /flash/12345.cfg...

Download config file is success.

Start to parse config file /flash/startup...

Parse config file is success.

Execute python script success.
```

#Download the version and configuration file successfully, and then, auto restart the device via ZTP.

```
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345,script execute success

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12345,System will rebooted by DHCP upgrade
```

Device2:

#From the following logs, you can see that the device enters the ATP process and sends the DHCP request.

```
Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Now starting dhcp upgrade...
```

Apr 22 2020 06:03:58 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, DHCP discovery phase started...

#During the ZTP request period, you can exit the ZTP process through ctrl+c, so as to start with empty configuration. If you do not press Ctrl + C, you can continue to follow the ZTP process.

Apr 22 2020 06:04:00 Device1MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Press (ctrl + c) to abort Dhcp Upgrade

#Get the address successfully, and download the common intermediate file.

Apr 22 2020 06:04:35 Device1 MPU0 %DHCP-ASSIGNED_EXT-5:Interface vlan1 assigned DHCP address 1.0.0.5, mask 255.255.255.0.

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Dhcp discovery phase success

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Start to download temp file ztp.py...

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Download temp file ztp.py is success

Apr 22 2020 06:04:35 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340, Start to parse temp file...

#Directly execute the python script.

/flash free space is 101(M).

Start to get remote and local file path.

Get remote and local file path is success.

#Download the version.

Start to download image file /flash/ztp.pck...

Download image file is success

Start to set boot image file /flash/ztp.pck....

#Download and analyze the stacking file and configuration file.

Start to download stack file /flash/12340.stack...

Download stack file is success.

Start to download config file /flash/12340.cfg...

Download config file is success.

Start to parse config file /flash/startup...

Parse config file is success.

Execute python script success.

#Download the version and configuration file successfully, and then, auto restart the device via ZTP.

Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340,script execute success

```
Apr 22 2020 06:12:26 Device1 MPU0 %ZTP-DHCP_UPGRADE-5:SerialNum:12340,System will
rebooted by DHCP upgrade
```

Step 5: Check the result.

#Check the ZTP status via the command **show ztp**. Execute the commands **show running-config** and **show version**, and you can see that the configuration and version take effect. Execute the command **show vst-config**, and you can see that the stacking takes effect.

```
switch#show ztp

Last ztp method: DHCP upgrade method
   Ztp state: ZTP DHCP upgrade success
   Ztp important inforamtion:
      FTP server IP: 1.0.0.2
      Temporary file name: ztp.py

Current ztp method: None upgrade method

Next ztp state: Next ztp state: disable(Stack mode does not support ztp.)

switch X#show vst-config
Building Configuration...

!mode member information
switch mode virtual
switch virtual member 0
 domain 101
exit
switch virtual member 1
 domain 101
 exit
!mode member end


!mode vsl information
vsl-channel 0/1
 exit
vsl-channel 1/1
```

```
 exit
!mode vsl end


!slot_0_ SOFOS SFN3300 24P4X(V1)
!vsl  mode
!slot 0/0
interface tengigabitethernet0/0/50
 vsl-channel 0/1 mode on
 exit
!end

!slot_14_ SOFOS SFN3300 24P4X(V1)
!vsl  mode
!slot 1/0
interface tengigabitethernet1/0/50
 vsl-channel 1/1 mode on
 exit
!end
```

Note

- The device can obtain the file download mode through option66 of the DHCP protocol, and supports FTP, SFTP and TFTP. You can choose any download mode during configuration.
- The MD5 of version file, configuration file and stack file are stored separately, and the name is their own file plus the suffix .md5.
- When stacking automatically, the interface dimension in the configuration file must be the interface dimension after stacking, not the interface dimension when it is single machine.
- After downloading the python file, the device will execute the python file directly, so the python file must conform to the python syntax.
- If the version information is not found through the device sequence, the

ZTP process of the device will not upgrade the version, but will only load the configuration and continue the ZTP process, but the configuration file cannot be empty.

3 Interfaces

3.1 Interface Basis

3.1.1 Overview

The interfaces supported by the device can be divided to physical interface and logical interface. The physical interface includes L2 Ethernet interface and L3 Ethernet interface; logical interface includes aggregation group interface, VLAN interface, Loopback interface, Null interface, Tunnel interface and so on.

L2 Ethernet interface, also called 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.

L3 Ethernet interface is one physical interface and works in layer 3 in the OSI reference model-network layer. It can configure IP address and is mainly used to forward packets.

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.

Loopback interface, also called local loopback interface, is one logical interface. For the packets sent to the Loopback interface, the device regards that the packets are sent to the device itself, so it does not forward the packets.

Null interface is one logical interface. Any packet sent to Null interface is dropped.

Tunnel interface is one logical interface, providing the transmission link for the point-to-point mode.

For different interfaces, there are corresponding configuration modes. The related

configuration modes of the interfaces include:

- Interface configuration mode, corresponding to VLAN interface, Loopback interface, Null interface, and Tunnel interface
- L2 Ethernet interface configuration mode, corresponding to L2 Ethernet interface
- L3 Ethernet interface configuration mode, corresponding to L3 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.

3.1.2 Basic Function Configuration of Interfaces

Table 155 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
Configure the concerned layer of the interface status SNMP proxy	Configure the concerned layer of the interface status SNMP proxy

3.1.2.1 Configure Basic Functions of Interfaces

Configuration Conditions

No

Enable/Disable Interface

After the port is disabled, it cannot receive or send packets, but after the Ethernet interface is enabled, whether it can receive and send packets also depends on other setting, such as whether the peer Ethernet interface is enabled, the rates of the local and peer Ethernet interfaces, 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 156 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/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the virtual switch link interface mode, the subsequent configuration just takes effect on the current virtual switch link interface.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	
Enter the virtual switch link interface configuration mode	vsl-channel *vsl-channel-id*	

Step	Command	Description
Enable interface	no shutdown	Mandatory By default, the interface is enabled.
Disable interface	shutdown	Mandatory By default, the interface is enabled.

Note

- The Null interface does not support the function of configuring the interface description.

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 157 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	
Enter the virtual switch link interface configuration mode	vsl-channel *vsl-channel-id*	

Step	Command	Description
		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; after entering the virtual switch link interface mode, the subsequent configuration just takes effect on the current virtual switch link interface.
Configure interface description information	description *description-name*	Mandatory By default, the description information of the interface is not configured.
	peer-description *description-name*	Mandatory By default, do not configure the description information of the peer interface.

Note

- The Null interface does not support the function of configuring the interface description.

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 158 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; after entering the virtual switch link interface mode, the subsequent configuration just takes effect on the current virtual switch link interface.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	
Enter the virtual switch link interface mode	vsl-channel *vsl-channel-id*	
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.

Note

- The Null interface does not support the function of configuring the interface description.

3.1.2.2 Configure Interface Group Functions

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 Condition

The interfaces covered by the interface group should already exist.

Configure Interface Group

Table 159 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	configure terminal	-
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.

3.1.2.3 Configure Concerned Layer of Interface Status SNMP Proxy

In fact, the interface UP/DOWN status includes the status of two layers in the system. One is L2 link layer status and the other is L3 protocol layer status. You can use the **show ip interface brief** command to view. The two status change with the UP/DOWN change of the physical interface, but when configuring keepalive gateway on the Ethernet interface, L3 protocol layer status is controlled by the keepalive detection status.

If the SNMP proxy function is enabled on the device, the network management server can get the interface status information via the public mib and also can send the interface status change information to the network management server when SNMP Trap is enabled.

With the function command, you can set the concerned interface status layer of the SNMP proxy. By default, the concerned interface status layer of the SNMP proxy

is the L2 link layer, but when Ethernet interface configures keepalive gateway, to realize that the displayed interface status of the network management server links with the keepalive detection status consistently, it is necessary to set the concerned interface status layer of the SNMP proxy as L3 protocol layer. Therefore, in the environment enabled with the keepalive detection (such as MSTP WAN line environment), it is suggested to set link-status-care l3.

Configuration Condition

No

Configure Interface Group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the network management layer of the interface status	link-status-care { l2 | l3 }	Mandatory By default, the concerned layer of the interface status SNMP proxy is L2 link layer.
Enter the global configuration mode	exit	-

3.1.2.4 Basic Monitoring and Maintaining of Interfaces

Table 160 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.
show interface snmp ifindex	Display the SNMP NMS index values corresponding to all interfaces under the interface

3.2 Ethernet Interface

3.2.1 Overview

Ethernet interface includes L2 Ethernet interface and L3 Ethernet interface.

L2 Ethernet interface, also called 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:

Data frame forwarding: According to the MAC address (that is physical address) of the data frame, forward the data frame. L2 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.

MAC address learning: Construct and maintain the MAC address table, used to support forwarding the data frames.

L3 Ethernet interface is one physical interface. It works at layer 3 in the OSI reference model-data link layer. It is mainly used to execute two basic operations:

Packet forwarding: Perform the route forwarding of the packets according to the IP (Internet Protocol) address (that is net5work address) of the packet. L3 Ethernet interface can only perform the L3 route forwarding for the received packet, that is, can receive and send the packet whose source IP and destination IP are in different segments.

According to the maximum rate supported by the Ethernet interface, the Ethernet interface type can be divided to the following four:

fastethernet: 100M Ethernet interface can be abbreviated as Fa, such as fastethernet0/1 or Fa0/1;

gigabitethernet: 1000M Ethernet interface, can be abbreviated as Gi, such as gigabitethernet0/25 or Gi0/25;

tengigabitethernet: 10G Ethernet interface, can be abbreviated as Te, such as

tengigabitethernet1/1 or Te1/1.

25ge: 25G Ethernet interface;

40ge: 40G Ethernet interface;

According to the media type of the Ethernet interface, the Ethernet interface type can be divided to copper (electrical port) and fiber (optical port).

3.2.2 Ethernet Interface Function Configuration

Table 161 Function configuration list of Ethernet interface

Configuration Task	
Configure basic functions of the Ethernet interface	Enter the Ethernet interface configuration mode
	Enter the batch configuration mode of L2 Ethernet interface
	Configure the rate and duplex mode
	Configure FEC
	Configure MDIX (Media Dependent Interface Crossover) mode
	Configure the media type
	Configure MTU (Maximum Transmission Unit)
	Configure flow control
	Configure delay time
	Configure auto energy-saving
	Configure the energy efficient Ethernet function
	Configure the optical module type supported by the port
	Configure forcing to cancel the OMM-disabled state of the interface
Configure the Ethernet interface detection function	Configure the status flap detection
	Enable the loopback test
Configure storm suppression of L2 Ethernet interface	Configure the storm suppression parameter
	Configure the action executed after the storm suppression

Configuration Task	
Configure the UNI/NNI attribute	Configure the UNI/NNI attribute
	Configure the uni port connectivity
Configure the basic functions of the L3 Ethernet interface	Configure the L3 Ethernet interface

3.2.2.1 Configure Basic Functions of Ethernet Interface

Configuration Condition

No

Enter Ethernet Interface Configuration Mode

To configure on the specified port, first enter the L2 Ethernet interface configuration mode of the Ethernet interface or L3 Ethernet interface configuration mode and then execute the corresponding configuration command.

Table 162 Enter the L2 Ethernet interface configuration mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Mandatory After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.

Note

- The naming rule of the Ethernet interface number is U/S/P (Unit/Slot/Port). Unit indicates the device in the stacking state, numbered from 0. When the device is initialized, it is necessary to confirm whether the device is in the

stacking state. If no, the device number is 0 and hidden by default. 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 Ethernet interface on the device or interface card. The Ethernet interface on each device and interface card is numbered from 1.

- The naming rule of the Ethernet interface name *interface-name* is Ethernet interface type + Ethernet interface number. For example, gigabitethernet0/1 indicates the 1000M Ethernet interface numbered 1; tengigabitethernet1/2 indicates the Gigabit Ethernet interface numbered 2 on the service slot numbered 1. In the VST mode, gigabitethernet0/1/2 indicates 1000M Ethernet interface numbered 2 on the service slot numbered 1 of the member device numbered 0.

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 163 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

Note

- L3 Ethernet interface does not support the batch configuration mode.

Configure Rate and Duplex Mode

Setting the rate of the Ethernet interface includes two cases:

One is to set the fixed rate according to the Ethernet interface rate capability set. The optional parameters include **10** (10M), **100** (100M), **1000** (1000M), **10000** (10000M), 25000 (25000M), and 40000(40000M).

The other is to set the rate as auto (auto-negotiation), specifying that the rate is negotiated by the local and peer Ethernet interfaces.

Similarly, setting the duplex mode of the Ethernet interface includes two cases:

One is to set the duplex mode of the Ethernet interface according to the capability set of the Ethernet interface duplex mode. The optional parameters include full (full-duplex mode), indicating that the Ethernet interface can send packets when receiving the packets; half (half-duplex mode), indicating that the Ethernet interface 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 and peer Ethernet interfaces.

Table 164 Configure the rate and duplex mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface interface-name	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration

Step	Command	Description
		just takes effect on the current interface.
Configure the rate of the Ethernet interface	speed { 10 | 100 | 1000 | 10000 | |25000|40000|auto }	Mandatory
Configure the duplex mode of the Ethernet interface	duplex { auto | full | half}	Mandatory

Note

- When the Ethernet interface 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 Ethernet interface 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 and 10000M, and the supported duplex mode is auto and full-duplex mode.

Configure FEC

FEC (forward error correction) is a kind of error correction method. It can improve the signal quality by adding error correction information to the packet at the sending port and using error correction information to correct the error code generated during the transmission of the packet at the receiving end, but it will also bring some delay to the signal. The user can choose to disable or enable this function according to the actual situation.

The FEC status of the port can be configured manually or in an adaptive way. If the user does not configure the supported optical module type on the port, when inserting the module or configuring the port rate, the FEC will be configured adaptively according to the module type and rate inserted in the current port. If there is user configuration on the port, it will be subject to user configuration and will not be

adaptive when the port is inserted into the module or configured with speed.

Table 165 Configure the port FEC status

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface interface-name	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure the port FEC status	[no] fec mode {base-r {auto|manual} |rs { auto|manual }|none manual}	Mandatory By default, the port does not enable FEC.

Note

- When the rate is not 25G or 100G, FEC cannot be configured. When the port has manual configuration of FEC, you cannot switch the rate to non-25G or 100G.
- This function cannot be configured on the VSL member port.
- Auto is configured to be distributed adaptively. Before restarting the device, the user needs to use the write command to save the configuration.
- Only 25GE and 100GE interfaces support this function. FEC configuration will take effect only when the actual speed is 25G or 100G.

Configure MDIX Mode

The signals can be sent only after the local and the peer Ethernet interfaces are connected. Therefore, the MDIX mode is used with connection cables.

The cables connecting Ethernet interfaces 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 only supports straight-through cable.

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 Ethernet interfaces cannot be the same.

When using crossover cable, the MDIX modes of the local and peer Ethernet interfaces should be the same or at least one is auto.

Table 166 Configure the MDIX mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
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.

Note

- The optical port does not support the configuration.

Configure Media Type

Switch to use the optical port or electrical port on the Combo port by configuring the media type of the Ethernet interface. The optical port and the corresponding electrical port cannot work at the same time. When specifying one media type on Combo port, the other media type is automatically disabled.

Table 167 Configure media type

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure media type	media-type { auto | copper | fiber }	Mandatory By default, the media type of the electrical port is copper; the media type of the optical port is fiber; the media type of the Combo port is copper.

Note

- When switching the optical port and electrical port on the Combo port, the Ethernet interface configuration after switching, such as rate, duplex mode,

and MDIX mode, are initialized to the default values.

Configure MTU

The MTU configured on the L2 Ethernet interface 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 takes effect for the ingress and egress packets. When the length of the packet sent by the local device 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 168 Configure MTU

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure MTU	mtu *mtu-value*	Mandatory By default, the MTU of L2 Ethernet interface is 1824 bytes and the MTU of L3 Ethernet interface is 1500 bytes.

Configure 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 169 Configure flow control

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure flow control	flowcontrol { on | off }	Mandatory By default, the flow control function of the port is disabled.

Note

- The local flow control can be realized only when the local and peer ends both enable the flow control function.
- L3 Ethernet interface does not support flow control.

Configure Delay Time

When the port changes from Up to Down or from Down to Up, 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 170 Configure delay time

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface	interface *interface-name*	-

Step	Command	Description
configuration mode		
Configure delay time	link-delay { up-hold-time | down-hold-time } *link-delay-value*	Mandatory By default, the delay reporting function is not enabled. When the up and down status of the port changes, it is reported and processed immediately.
Disable delay reporting	no link-delay { up-hold-time | down-hold-time }	

Configure 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 171 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 auto energy-saving	auto-power-down enable	Mandatory By default, the auto energy-saving function of the port is disabled.

Note

- L3 Ethernet interface does not support configuring auto energy-saving.

Configure Energy Efficient Ethernet Function

When no data traffic passes, the Ethernet interface inside is always polling the port state. To reduce such unnecessary consumption, you can configure the 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 172 Configure the energy efficient Ethernet function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure the energy efficient Ethernet function	energy-efficient-ethernet enable	Optional By default, the energy efficient Ethernet function of the Ethernet interface is disabled.

Note

- After the Ethernet 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 the 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.

Configure Optical Module Type Supported by Port

The Gigabit and 10G Ethernet optical interfaces are in the OMM-disabled state when the optical modules are not inserted. This port can be enabled only when the type of optical module inserted on the port is the same as that supported by the port configuration. Therefore, you need to configure the type of optical module supported by the port, which can be manually configured by the user or configured in an adaptive way. If the user does not configure the supported optical module type on the port, the optical module type supported by the port will be adaptively configured according to the module type inserted on the port, so that the port can use the corresponding optical module normally. If there is a user configuration on the port, it will be subject to the user configuration and will not be adaptive according to the type of module inserted in the port.

The types of optical modules include Gigabit photoelectric module, 10G photoelectric module, common optical module, and unrecognized optical module. The common optical modules include Gigabit optical module, 10G Optical module, 10G high-speed cable, 40G optical module, 40G high-speed cable and other optical modules. Unrecognized optical modules cannot be used normally.

By default, the port supports common optical modules.

Due to the different speed capability levels supported by different types of modules, when the configuration port supports different optical module types (including user configuration and adaptive configuration), the speed configuration of the port may be modified synchronously.

Table 173 Configure the optical module type supported by the port

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3

Step	Command	Description
		Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure the optical module supported by the port	optical fiber-to-copper { get | xget }	Mandatory By default, the port supports the common optical module.
Clear the configuration of the optical module type supported by the port	no optical fiber-to-copper { get [auto] | xget [auto] | unknown-module auto }	Mandatory The auto command is used to clear the self-adaptive configuration, but cannot clear the user configuration. After the self-adaptive configuration is cleared, the port supports the common optical module by default. At this time, the self-adaptive will be triggered only after the optical module is swapped or the device is restarted. The non auto command is used to clear the user configuration and will automatically re-adapt according to the type of optical module inserted on the port.

Note

- You can configure the function only on the Ethernet optical interface, but cannot configure on the electrical port or combo port.
- This function cannot be configured on the VSL member port.
- The function cannot be configured on 40G or 100G port.
- Auto is configured to be distributed adaptively. Before restarting the device, the user needs to use the write command to save the configuration.

Configure Forcing to Cancel OMM-disabled State of the Interface

When the Ethernet optical interface is not inserted into the optical module, the port will be in the OMM-disabled state, unable to receive and send packets. After inserting a valid optical module, the OMM disabled state of the Ethernet optical interface will be automatically cancelled. However, sometimes the Ethernet port can also be up without the optical module inserted, such as enabling the loopback detection function. At this time, you can configure to forcibly cancel the OMM disabled state of the Ethernet optical interface.

Only when the optical module is not inserted to Ethernet optical interface, it will be in the OMM disabled state. The electric interface and combo interface will not be set to the OMM disabled state, so this function is unnecessary.

Table 174 Configure forcing to cancel the OMM-disabled state of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration

Step	Command	Description
		just takes effect on the current interface.
Enable forcing to cancel the OMM-disabled state of the interface	optical enable port manual	Mandatory By default, the function is disable.
Disable forcing to cancel the OMM-disabled state of the interface	no optical enable port manual	Mandatory By default, the function is disable.

Note

- You can configure the function only on the Ethernet optical interface, but cannot configure on the electrical port or combo port.
- This function cannot be configured on the VSL member port.

Configure Port crc Error Packet Detection Function

It is necessary to configure snmp-server enable traps crc-error first. This function is used to count whether CRC error packets within the *time-value* time range exceed the upper limit. If it exceeds the upper limit, an alarm trap will be sent. When the number of CRC error packets is recovered from higher than the upper limit to lower than the lower limit, the recovered trap will be sent.

Table 175 Configure the crc error packet detection function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface configuration mode/aggregation group configuration mode	interface *interface-name*	Mandatory After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current

Step	Command	Description
		interface.
Configure the crc error packet detection trap function	crc-error max-limit max-value min-limit min-value interval *time-value*	Mandatory By default, the function of sending trap when the crc error packet statistics of the port exceeds the alarm range is disabled. max-value: The maximum number of the port crc error packets min-value: The minimum number of the port crc error packets time-value: Set the detection time range, and the unit is second
Disable the crc error packet detection function	no crc-error	Mandatory By default, the function is disabled.

Configure the Function of Logging Port Detecting crc Error Packet

This function is used to count whether CRC error packets within the *time-value* time range exceed the upper limit. If it exceeds the upper limit, an alarm trap will be sent. When the number of CRC error packets is recovered from higher than the upper limit to lower than the lower limit, record the recovery log, which needs to be used with the port crc error packet detection function at the same time.

Table 176 Configure the crc error packet detection recording log function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the function of logging crc error packet detection	crc-error logging	Mandatory By default, the function is disabled.
Disable the function of logging crc	no crc-error logging	

Step	Command	Description
error packet detection		

Configure Port Error Packet Detection Function

It is necessary to configure snmp-server enable traps { in-packet-error | out-packet-error } first. This function is used to count whether port error packets within the *time-value* time range exceed the upper limit. If it exceeds the upper limit, an alarm trap will be sent. When the number of port error packets is recovered from higher than the upper limit to lower than the lower limit, the recovery trap will be sent.

Table 177 Configure the error packet detection function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Mandatory After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current interface.
Enable error packet detection trap function	packet-error {in-packet | out-packet} max-limit *max-value* min-limit *min-value* interval *time-value*	Mandatory By default, the error packet statistics of the port exceeds the alarm range, the function of sending the trap is disabled. in-packet: Enable the trap function for the number of ingress error packets of the port. out-packet: Enable the trap function for the number of egress error packets of the port. max-value: The upper limit value of port error packets. min-value: The lower limit value of port error packets.

Step	Command	Description
		time-value: Set the detection time range, in the unit of seconds.
Disable error packet detection trap function	no packet-error {in-packet | out-packet}	Mandatory By default, the function is disabled.

Configure the Function of Logging Port Detecting Error Packet

This function is used to count whether error packets within the *time-value* time range exceed the upper limit. If it exceeds the upper limit, record the alarm log. When the number of error packets within the *time-value* time range is recovered from higher than the upper limit to lower than the lower limit, record the recovery log, which needs to be used with the port error packet detection function at the same time.

Table 178 Configure the error packet detection recording log function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the function of logging error packet detection	packet-error { in-packet | out-packet } logging	Mandatory By default, the function is disabled.
Disable the function of logging error packet detection	no packet-error { in-packet | out-packet } logging	

Configure Port Traffic Exceeding Bandwidth Function

You need to configure snmp-server enable traps {in-usage-rate | out-usage-rate }. This function is used to send an alarm trap when the ingress/egress bandwidth utilization rate of the port exceeds the upper limit. When the ingress/egress bandwidth utilization rate of the port recovers from higher than the upper limit to lower than the lower limit, the recovered trap will be sent.

Table 179 Configure the port traffic exceeding bandwidth function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface/aggregation group configuration mode	interface *interface-name*	Mandatory After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Configure the port traffic exceeding bandwidth trap function	flow-warn { in-packet | out-packet } max-usage *max-value* min-usage *min-value*	Mandatory By default, the function of sending trap when the port traffic exceeds the bandwidth is disabled. in-packet: Enable the ingress bandwidth utilization trap function of the port. out-packet: Enable the egress bandwidth utilization trap function of the port. max-value: The maximum value of the bandwidth utilization min-value: The minimum value of the bandwidth utilization
Disable the traffic exceeding bandwidth trap function	no flow-warn {in-packet | out-packet}	Mandatory By default, the function is disabled.

Configure the Function of Logging Port Traffic Exceeding Bandwidth

This function is used to record the alarm log when the ingress/egress bandwidth utilization of the port exceeds the upper limit, and the recovery log when the ingress/egress bandwidth utilization of the port recovers from above the upper limit to

below the lower limit.

Table 180 Configure the function of logging port traffic exceeding bandwidth

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the function of logging port traffic exceeding bandwidth	flow-warn { in-packet | out-packet } logging	Mandatory By default, the function is disabled.
Disable the function of logging port traffic exceeding bandwidth	no flow-warn { in-packet | out-packet } logging	

Configure the Port Single Fiber Function

Configure the single fiber function of the Ethernet interface, which configures the Ethernet interface to support sending and receiving packets at the same time in single fiber mode.

Table 181 Configure the single-fiber function of the port

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Mandatory After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current interface.
Configure the single-fiber function	single-fiber mode	Mandatory By default, the single-fiber function of the Ethernet interface is disabled. Enable the single-fiber sending and receiving function.

Step	Command	Description
Disable the single-fiber function	no single-fiber mode	Mandatory By default, the function is disabled.

Note

- The single fiber command can only be used when the Ethernet interface type is optical port
- Enable the single fiber function. The port can be up without negotiation. It is necessary to ensure that the rates at both ends are consistent in order to communicate normally.

3.2.2.2 Configure Ethernet Interface Detection Function

Configure Status Flap Detection

When the Ethernet interface 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 Ethernet interface or called Link-Flap and the Ethernet interface is automatically disabled and set as Error-Disabled.

Table 182 Configure status flap detection

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure flap detection	errdisable flap-setting cause link-flap max-flaps *max-flaps-number* time *time-value*	Mandatory By default, the trigger condition of executing Link-Flap is: within 10s, the detected Ethernet interface becomes Up

Step	Command	Description
		for at least 5 times.

Note

- When the Ethernet interface 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 Loopback Test

When performing some troubleshooting, such as locating the Ethernet interface fault initially, you can enable the Ethernet interface loopback test function. The Ethernet interface enabled with the loopback test function cannot forward packets normally.

The loopback test function of the Ethernet interface includes internal loopback test and external loopback test.

During internal loopback test, change the internal receiving end and sending end of the specified Ethernet interface to make the packets sent by the Ethernet interface loopback in the device and received by the Ethernet interface. If the internal loopback test succeeds, it indicates that the Ethernet interface inside works normally. The Ethernet optical interface will be in the OMM-disabled state when it is not inserted with the optical module, and the configured internal loop cannot be UP. At this time, the port OMM-disabled state needs to be cancelled first.

During the external loopback test, first insert one self-loop cable on the Ethernet interface and the packets sent by the specified Ethernet interface return to the Ethernet interface via the self-loop cable and received by the Ethernet interface. If the external

loopback test succeeds, it indicates that the Ethernet interface works normally.

Table 183 Enable loopback test

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current interface.
Enable loopback test	loopback { internal | external }	Mandatory By default, the loopback test function of the Ethernet interface is not enabled.

Note

- The device does not support the external loopback test function.

3.2.2.3 Configure Storm Suppression of L2 Ethernet Interface

Configure Storm Suppression Parameters

Limit the broadcast, multicast or unknown unicast traffic on the port by configuring the storm suppression parameters. When the broadcast, unknown 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 184 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* | kbps *bps-value* | pps *pps-value* }	Mandatory By default, do not configure the port storm suppression.

Note

- L3 Ethernet interface does not support the storm suppression parameter.

Configure Action Executed after Storm Suppression

When the storm is detected on the specified port and the storm suppression is enabled, you can select three policies to process the storms on the port:

One is to record on the device and print and output the detected storm alarm information on the terminal. In the mode, the port is still enabled, so the port can receive the subsequent traffic and the storm on the port cannot be removed.

One is to disable the port, record on the device and print and output the detected storm alarm information on the terminal, and send the alarm information of detecting the 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.

Another is to record on the device and print and output the detected storm alarm information on the terminal, and 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 185 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 executed after the interface detects the storm is to record on the device and print and output the detected storm alarm information on the terminal.

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**.
- L3 Ethernet interface does not support configuring the action executed after storm suppression happens.

3.2.2.4 Configure Broadcast Packet Shielding

Unknown unicast packets, unknown multicast packets and broadcast packets will be broadcasted in VLAN. In some applications, the port does not need to send these packets. If the broadcast packet shielding function is enabled under these ports, these ports will not send these packets. This function takes effect in the outgoing direction of the port.

Configuration Conditions

None

Configure Broadcast Packet Shielding

Table 186 Configure broadcast packet shielding

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure broadcast packet shielding	flood-control { bcast | unknown-mcast | unknown-ucast }	Mandatory By default, broadcast packets, unknown multicast packets and unknown unicast packets are not shielded at the outgoing port

3.2.2.5 Configure UNI/NNI Type

Configure 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 187 Configure UNI/NNI attribute

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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the UNI/NNI attribute	port-type { nni | uni }	Mandatory By default, the UNI/NNI type of the L2 Ethernet interface and aggregation group is nni.

Note

- L3 Ethernet interface does not support configuring the UNI/NNI type.

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 188 Configure the connectivity of uni port

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface	interface *interface-name*	Either

Step	Command	Description
configuration mode		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	interface link-aggregation *link-aggregation-id*	
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.
- L3 Ethernet interface does not support configuring the connectivity of the uni port.

3.2.2.6 Configure Basic Functions of L3 Ethernet Interface

According to the processing layer of the Ethernet interface for the packet, Ethernet interface can work in the L2 mode or L3 mode. If setting the work mode of the Ethernet interface as the L2 mode, it is used as one L2 Ethernet interface. If setting the work mode of the Ethernet interface as L3 mode, it is used as one L3 Ethernet interface and its role is equivalent to the VLAN interface.

Configuration Condition

No

Configure Reserved vlan

Table 189 Configure reserved vlan

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure reserved vlan	vlan reserved for routedport *vlan-list*	The value range of *vlan-list* is 2-4094. By default, do not create reserved vlan.

Configure L3 Ethernet Interface

Table 190 Configure L3 Ethernet interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the L3 Ethernet interface	no switchport [reserved-vlan]	Mandatory reserved-vlan: The interface mode of the reserved VLAN By default, Ethernet interface works in the L2 mode and is used as one L2 Ethernet interface.
Enter the L3 Ethernet sub interface configuration mode	interface *interface-name*	Mandatory To enter the L3 Ethernet sub interface configuration mode, you need to create the corresponding L3 Ethernet interface first. By default, there is no L3 Ethernet sub interface.

Note

- After the work mode of Ethernet interface switches, the other configurations of the Ethernet interface except for description, shutdown, speed, duplex, media-type, mdix, eee, all restore to the default configuration in the new mode.
- When the Ethernet interface serves as one L3 interface, for the configuration of the L3 Ethernet interface basic functions, refer to the configuration of VLAN interface basic functions.
- To switch the L2 Ethernet interface to the L3 Ethernet interface with reserved VLAN, you need to create reserved VLAN first.
- For the conversion between common L3 interface and reserved VLAN L3 interface, you need to switch to the L2 interface first, and then switch to the required L3 interface mode.

3.2.2.7 Ethernet Interface Monitoring and Maintaining

Table 191 Ethernet interface monitoring and maintaining

Command	Description
clear interface *interface-name*	Clear the statistics information of the specified L3 Ethernet interface
clear interface { *interface-list* | switchport } statistics	Clear the packet and traffic statistics information of the port
clear optical { all | interface *interface-list* } exception statistic	Clear the abnormality statistics information of the optical module inserted on the Ethernet interface
show errdisable flap-values	Display the current setting of triggering executing Link-Flap function
show interface { *interface-list* [group] |	Display all information or abstract information

Command	Description
switchport [brief [down | up | vsl]] }	of the Ethernet interface or virtual switch link member port
show interface *interface-list* statistics	Display the packet and traffic statistics information of the port
show interface switchport statistics [packet | rate | ratio]	Display the packet and traffic statistics information of all ports on the device
show interface all statistics [packet | rate | ratio]	Display the packet and traffic statistics of all L2 interfaces and L3 interfaces of the device
show optical { all | interface *interface-list* } [detail | exception statistic]	Display the information of the optical module inserted on the Ethernet interface
show port-type [*interface-list* | { uni | nni } [interface *interface-list*]]	Display the UNI/NNI attribute information of the port
show group-port	Display the attribute information of the same group to which the Ethernet interface belongs
show interface *interface-list* rate-peak [input | output]	Display the flow monitoring information of the specified port
show storm-control [interface *interface-list*]	Display the storm suppression setting of the specified port
show optical { all | interface *interface-list* } omm-disabled status	Display whether the port is in the OMM-disabled state and the reason why the port is in the OMM-disabled state
show routedport reserved-vlan	Display the usage of reserved VLANs in the L3 Ethernet interface
show routedport interface { all | *interface-list* }	Display the configuration status of the L3 Ethernet interface

3.2.3 Typical Configuration Example of Ethernet Interface

3.2.3.1 Configure Storm Suppression Function

Network Requirements

Configure the storm suppression function on the port of the device to suppress the broadcast, unknown unicast and unknown multicast packets, realizing that PC2 can

access Internet normally when PC1 sends lots of broadcast, unknown unicast and unknown multicast packets.

Network Topology

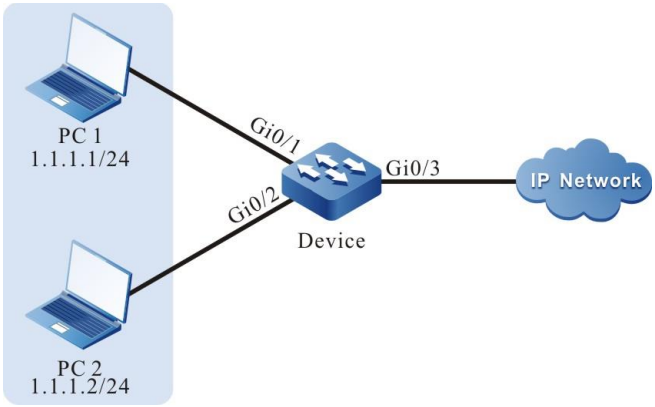


Figure 43 Network topology of configuring storm suppression

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 unknown multicast packets on port gigabitethernet0/1 and the suppression rate is 1024bps.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control broadcast kbps 1024
Device(config-if-gigabitethernet0/1)#storm-control unicast kbps 1024
Device(config-if-gigabitethernet0/1)#storm-control multicast kbps 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
Status Codes: U - unicast, B - broadcast, M - multicast
 Interface        Unicast    Broadcast  Multicast  Action    Status
 ---------------------------------------------------------------------------
 gi0/1          1024kbps   1024kbps   1024kbps   logging   -|-|-
```

#When PC1 sends lots of broadcast, unknown unicast and unknown multicast packets, PC2 also can access Internet normally.

3.3 Aggregation Group Interface

3.3.1 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.

3.3.2 Aggregation Group Interface Function Configuration

Table 192 Function configuration list of aggregation group interface

Configuration Task	
Configure the basic functions of the aggregation group interface	Enter the aggregation group configuration mode
	Configure the aggregation group forwarding mode

3.3.2.1 Configure Basic Functions of L3 Aggregation Group Interface

Configuration Condition

No

Configure Reserved VLAN

Table 193 Configure the reserved VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the reserved VLAN	vlan reserved for routedport *vlan-list*	*vlan-list*: The value range is 2-4094 By default, do not create the reserved vlan.

Configure L3 Aggregation Group Interface

Table 194 Configure the L3 aggregation group interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	Mandatory
Configure the L3 aggregation group interface	no switchport [reserved-vlan]	Mandatory reserved-vlan: reserved VLAN interface mode By default, the aggregation Ethernet interface works in L2 mode and is used as a L2

Step	Command	Description
		Ethernet aggregation interface
Enter the L3 aggregation group sub interface configuration mode	interface *interface-name*	Mandatory To enter the L3 aggregation group sub interface configuration mode, you need to create the corresponding L3 aggregation group interface first By default, there is no L3 aggregation group sub interface

Note

- Before entering the specified aggregation group configuration mode, you must first create the corresponding aggregation group.
- After the working mode of the aggregation group interface is switched, all the other configurations of the aggregation group interface except for description and shutdown configuration will be restored to the default configuration in the new mode.
- When the aggregation group interface is used as a L3 interface, please refer to the configuration of the basic functions of VLAN interface for the configuration of the basic functions of the L3 Ethernet interface.
- To switch the L2 aggregation group interface to the L3 aggregation group interface of the reserved VLAN, you need to create reserved VLAN first.
- For the conversion between common L3 aggregation group interface mode and reserved VLAN L3 aggregation group interface mode, you need to switch to the L2 aggregation group interface mode first, and then switch to the required L3 aggregation group interface mode.

3.3.2.2 Monitoring and Maintaining of Aggregation Group Interface

Table 195 Monitoring and maintaining of aggregation group interface

Command	Description
clear interface switchport link-aggregation *link-aggregation-id* statistics	Clear the packet and traffic statistics information of the specified aggregation group
show interface switchport link-aggregation [*link-aggregation-id* | brief]	Display all information of the aggregation group
show interface link-aggregation *link-aggregation-id* statistics	Display the packet and traffic statistics information of the specified aggregation group
show interface link-aggregation *link-aggregation-id* rate-peak [input | output]	Display the flow monitoring information of the specified aggregation group
show port-type interface link-aggregation *link-aggregation-id*	Display the UNI/NNI attribute information of the aggregation group
show routedport reserved-vlan-	Display the usage of the reserved VLAN in the L3 aggregation group interface
show routedport interface link-aggregation *link-aggregation-id*	Display the configuration status of the L3 aggregation group

3.4 VLAN Interface

3.4.1 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.

3.4.2 VLAN Interface Function Configuration

Table 196 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
	Configure the up/down state of the configuration interface to be bound with the spanning tree state of its member port

3.4.2.1 Configure Basic Functions of VLAN Interface

Configuration Condition

No

Configure VLAN Interface

Table 197 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 198 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 199 Configure interface delay

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface vlan *vlan-id*	-
Configure VLAN interface delay	delay *delay-time*	Optional By default, the delay of the VLAN interface is 10 and the

Step	Command	Description
		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 200 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.

Configure the UP/DOWN State of the Interface to Be Bound with Spanning Tree State of Its Member Port

The up and down of the interface are bound to the link up/down status of its VLAN member port by default. At least one member port link is up, and the interface is up; All member port links are down, and the interface is down.

In some cases, the VLAN interface needs to care about the STP status of the member port, in which the STP status of at least one member port is forwarding, and the interface is up; Only when the STP status of all member ports is not forwarding can the interface be DOWN.

Table 201 Configure the up/down state of the configuration interface to be bound with the spanning tree state of its member port

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the up/down state of the configuration interface to be bound with the spanning tree	link-interface-vlan care stp	Mandatory By default, the UP/DOWN state of all VLAN interfaces are bound

Step	Command	Description
state of its member port		with the actual link state of its member port.

3.4.2.2 VLAN Interface Monitoring and Maintaining

Table 202 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

3.4.3 Typical Configuration Example of VLAN Interface

3.4.3.1 Configure VLAN Interface

Network Requirements

Configure the VLAN interface on Device to realize the intercommunication between PC1 and PC2 of different VLANs.

Network Topology

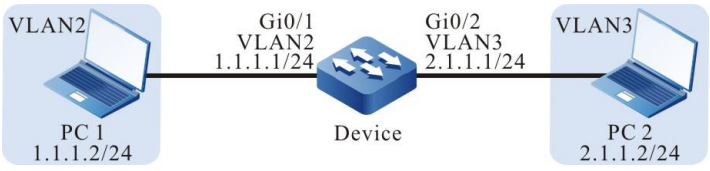


Figure 44 Network topology of configuring VLAN interface

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
    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
    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.
```

3.5 Loopback Interface

3.5.1 Overview

Loopback interface, also called local loopback interface, is one logical virtual interface realized by software. The interface is not affected by the physical status. As long as not disabling manually, its status is always enabled. In the dynamical routing protocol, such as OSPF, you can select the IP address of Loopback interface as Router ID. For the packets sent to the Loopback interface, the device regards that the packets are sent to itself, so it does not forward the packets.

3.5.2 Loopback Interface Function Configuration

Table 203 Function configuration list of Loopback interface

Configuration Task	
Configure the basic functions of Loopback interface	Configure loopback interface
	Configure the logical bandwidth of the interface
	Configure the interface delay

3.5.2.1 Configure Basic Functions of Loopback Interface

Configuration Condition

No

Configure Loopback Interface

Table 204 Configure Loopback interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create Loopback interface	interface loopback *unit – number*	Mandatory By default, do not create Loopback interface.

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 205 Configure the logical bandwidth of the interface

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

Step	Command	Description
mode		
Configure the logical bandwidth of the interface	bandwidth *width-value*	Optional By default, the logical bandwidth of Loopback interface is 8,000,000 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 206 Configure interface delay

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure interface delay	delay *delay-time*	Optional By default, the delay of the Loopback interface is 5000 and the unit is 10 ms.

3.6 Null Interface

3.6.1 Overview

Null interface is one logical interface realized by software. Any packet sent to Null interface is dropped. The dynamic routing protocol, such as OSPF, generates the auto-summarized route. The egress interface points to Null interface and can avoid route loop effectively. Null0 interface is created by the device by default and the user cannot disable or delete it.

3.6.2 Null Interface Function Configuration

Table 207 Function configuration list of Null interface

Configuration Task	
Configure the basic functions of Null interface	Configure the basic functions of Null interface

3.6.2.1 Configure Basic Functions of Null Interface

Configuration Condition

No

Configure Basic Functions of Null Interface

Table 208 Configure basic functions of Null interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter Null interface configuration mode	interface null 0	Mandatory
Configure prohibiting sending the error packet of ICMP unreachable	no ip unreachables	Optional By default, prohibit sending the error packet of ICMP unreachable.

Note

- Null interface just supports configuring permitting or prohibiting sending the error packet of ICMP unreachable.
- The packet reaching Null interface is dropped and it is not necessary to send the error of ICMP unreachable.

3.7 VSL Interface

3.7.1 Introduction to VSL Interface

Bind multiple physical ports to form one virtual switch link interface (VSL-

Channel). VSL channel is the logical link channel of exchanging the protocol packets and forwarding service data between the member switches in the VSL system. Each physical port is called the member port of the virtual switch link.

The member switches are added to one switch domain and they are interconnected via the VSL interface, forming one virtual switch.

3.7.2 VSL Interface Function Configuration

Table 209 The configuration list of the VSL channel functions

Configuration Task	
Configure the VSL channel functions	Enter the VSL channel configuration mode

3.7.2.1 Configure VSL Interface Function

Configuration Condition

No

Enter VSL Interface Configuration Mode

Table 210 Enter the VSL channel configuration mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VSL channel configuration mode	vsl-channel *vsl-channel-id*	Mandatory In the standalone mode, *vsl-channel-id* is one-dimension value, indicating the VSL channel number; in the VST mode, it is the two-dimension value. The first dimension is the virtual switch member number and the second dimension is the VSL channel number.

Note

Before entering the VSL channel configuration mode, first create the corresponding VSL channel.

3.7.2.2 VSL Interface Monitoring and Maintaining

Table 211 VSL interface monitoring and maintaining

Command	Description
clear vsl-channel *vsl-channel-id* statistics	Clear the packet and flow statistics information of the specified VSL interface
show vsl-channel *vsl-channel-id* rate-peak [input | output]	Display the flow monitoring information of the specified VSL interface
show vsl-channel *vsl-channel-id* statistics	Display the packet and flow statistics information of the specified VSL interface

3.8 Tunnel Interface

3.8.1 Overview

Tunnel is the technology of using one network protocol to transmit another network protocol. It includes the process of encapsulating, transmitting, and de-encapsulating data. The path passed by the encapsulated packet when being transmitted in the network is called tunnel. Tunnel is one virtual point-to-point connection. The devices at the two sides of the tunnel are called tunnel endpoints and they are responsible for encapsulating and de-encapsulating packets.

3.8.2 Tunnel Interface Function Configuration

Table 212 Function configuration list of tunnel interface

Configuration Task	
Configure the basic functions of the tunnel interface	Configure the basic functions of the tunnel interface

3.8.2.1 Configure Tunnel Interface

Configuration Condition

None

Configure Basic Functions of Tunnel Interface

Table 213 Configure basic functions of tunnel interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create tunnel interface and enter its configuration mode	interface tunnel *tunnel-unit*	Mandatory By default, the tunnel interface is not created on the device.
Configure work mode of tunnel interface	tunnel mode { gre[ip | ipv6] | ipip | ipipv6| ipv6ipv6 | ipv6ip [6to4 | isatap] }	Optional By default, the work mode of the tunnel interface is GRE over IPv4.
Configure TOS of tunnel interface	tunnel tos *tos-value*	Optional By default, the tunnel interface is not configured with TOS.
Configure TTL of tunnel interface	tunnel ttl *ttl-value*	Optional By default, the TTL value of the tunnel interface is 255.

Note

- The TOS configured on tunnel interface is used to fill the TOS field in the outer IPv4 packet header during encapsulation. If the TOS value is not configured on tunnel interface, use the TOS value in the inner IPv4 packet header.
- The TTL value configured on tunnel interface is used to fill the TTL field in the outer IPv4 packet header during encapsulation.

3.8.2.2 Tunnel Interface Monitoring and Maintaining

Table 214 tunnel interface monitoring and maintaining

Command	Description
enable	Privileged mode
debug tunnel {all | config | event | forward| packet }	Open the switch of the Tunnel debug information
show tunnel [*tunnel-id*] [slot *slot-num*]	Display the tunnel information

3.9 Loopback Group Interface

3.9.1 Overview

Loopback group interface is a logical virtual interface. Each loopback group interface includes a L2 Ethernet interface/L3 Ethernet interface/L2 static aggregation group/L3 static aggregation group. The port added to the loopback group is called the loopback port. The status of the loopback port is always enabled. For the packets sent to the loopback port, the device considers them to be sent to itself and will not forward the packets.

3.9.2 Loopback Group Interface Function Configuration

Table 215 Loopback group interface function configuration list

Configuration Tasks	
Configure the basic functions of the loopback group interface	Enter the global configuration mode
	Create loopback group
	Enter the L2 Ethernet interface configuration mode/L3 Ethernet interface configuration mode/aggregation group configuration mode
	Configure the loopback port or loopback aggregation group

3.9.2.1 Configure Basic Functions of Loopback Group Interface

Configuration Conditions

None

Configure Basic Functions of Loopback Group Interface

Table 216 Enter the aggregation group configuration mode

Step	Command	Description
Enter the global configuration mode	configure terminal	Mandatory
Create loopback group	`serviceloop-group` *`serviceloop-group-id`* `[description` *description-name*`]`	Mandatory
Enter L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the configuration mode of L2/L3 Ethernet interface, the subsequent configuration will only take effect on the current interface; After entering the aggregation group configuration mode, the subsequent configuration takes effect on all member ports of the aggregation.
Enter aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the loopback port	serviceloop-group *`serviceloop-group-id`* active	Mandatory

Note

- Before entering the specified aggregation group configuration mode, you must first create the corresponding aggregation group.
- Only L2 Ethernet interface, L3 Ethernet interface, L2 static aggregation group and L3 static aggregation group can be configured as loopback port.

3.9.2.2 Loopback Group Interface Monitoring and Maintaining

Table 217 Loopback group interface monitoring and maintaining

Command	Description
show serviceloop-group [*serviceloop-group-id*]	View the loopback group information
show serviceloop debug	View the enabled loopback group debug switch information
[no] debug serviceloop [config | event | sync | rpc | publisher]	Enable or disable the debug switch of the loopback group module

4 Ethernet Switching

4.1 Link Aggregation

4.1.1 Overview of Link Aggregation

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.

4.1.1.1 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 (LACPDUs) are used to interchange messages with the peer end.

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.

4.1.1.2 Link Aggregation Modes

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:

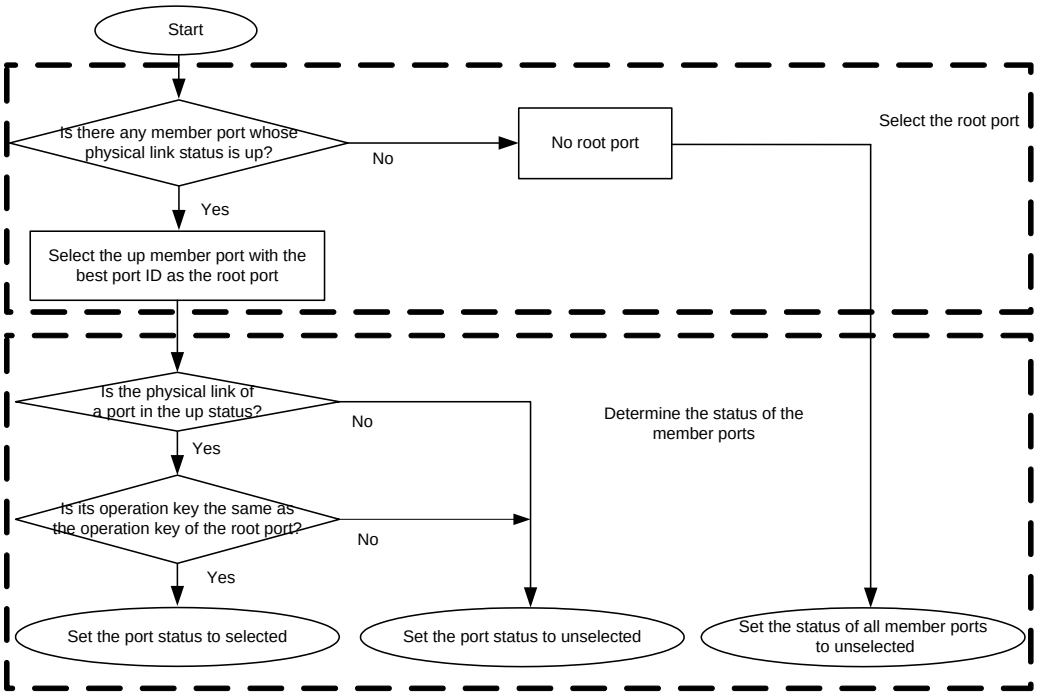


Figure 45 Setting the Status of Member Ports in Static Aggregation Mode

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 LACPDU 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:

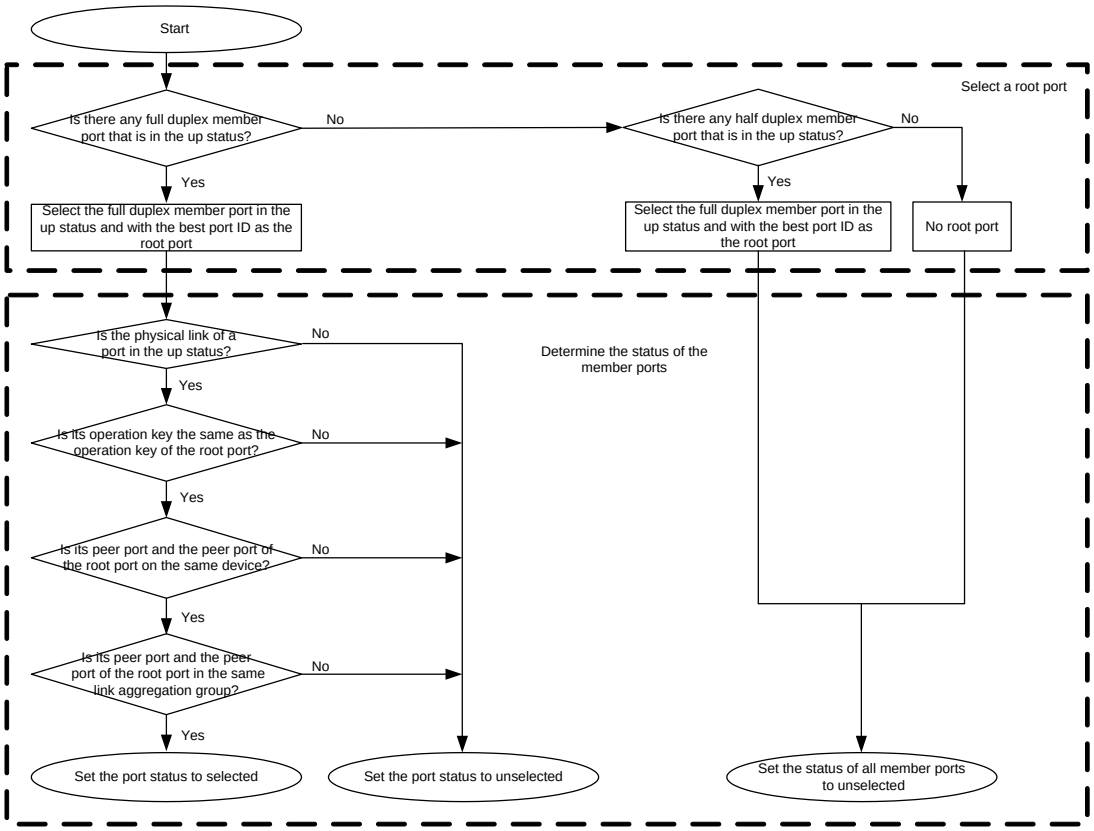


Figure 46 Setting the Status of Member Ports in Dynamic Aggregation Mode

4.1.1.3 Load Balancing Modes of Aggregation Groups

Seven load balancing modes are available, and users can select a mode according to the actual requirement.

- Load balancing based on the destination IP addresses: The aggregation group implements aggregated load balancing according to the destination IP addresses of packets.
- Load balancing based on the destination MAC addresses: The aggregation group implements aggregated load balancing based on the destination MAC addresses of packets.
- Load balancing based on the source and destination IP addresses: The aggregation group implements aggregated load balancing based on the source and destination IP addresses of packets.
- Load balancing based on the source and destination MAC addresses: The

aggregation group implements aggregated load balancing based on the source and destination MAC addresses of packets.

- Load balancing based on the source IP addresses: The aggregation group implements aggregated load balancing based on the source IP addresses of packets.
- Load balancing based on the source MAC addresses: The aggregation group implements aggregated load balancing based on the source MAC addresses of packets.
- Enhanced load balancing: If the number of ports that participates in user traffic forwarding is an odd number, this mode helps to improve the loading balancing capability of links with odd numbers. After configuring as the mode, the configuration of the load balancing profile adopted by the load balancing mode takes effect. If no load profile is created, adopt the default profile.

4.1.2 Overview of Load Balance Profile

4.1.2.1 Load Balance

Load-Balance means that when the egress of the traffic is the aggregation group, the chip can realize the load balance of the traffic between the member ports in the aggregation group according to the current HASH configuration conditions, so as to improve the bandwidth utilization of the aggregation group.

4.1.2.2 HASH KEY

HASH KEY means that when the traffic chooses the specific egress port of the aggregation group, the chip calculates the KEY value used by the port via HASH. Generally speaking, different packet types support different HASH KEY values, and different switch chips support different HASH KEY values. The HASH KEY values supported by different packets are shown in Table 1-1.

Table 218 The HASH KEY values supported by different packet types and their

meanings

HASH KEY Type	Description
dst-mac	Based on destination MAC address: Realize the aggregation load balance by the destination MAC address of the packet
src-mac	Based on source MAC address: Realize the aggregation load balance by the source MAC address of the packet
src-interface	Based on the receiving source interface: Realize the aggregation load balance by the receiving source interface of the packet
vlan	Based on VLAN: Realize the aggregation load balance by the VLAN of the packet
dst-ip	Based on destination IP address: Realize aggregation load balance by the destination IP address of the packet
l4-dst-port	Based on L4 destination port number: Realize aggregation load balance by the L4 destination port number of the packet
flow-label	Based on IPv6 flow label: Realize the aggregation load balance by the IPv6 flow label of the packet
protocol	Based on IP protocol: Realize the aggregation load balance by the IP protocol of the packet
src-ip	Based on source IP address: Realize aggregation load balance by the source IP address of the packet
l4-src-port	Based on L4 source port number: Realize aggregation load balance by the L4 source port number of the packet

In the local device, the HASH KEY values supported by different packets are shown in the following table:

Table 219 The HASH KEY values supported by different packets

Packet Type	Supported HASH KEY
L2 known unicast packet	dst-mac, src-mac, src-interface, vlan
L3 known unicast packet	dst-ip, l4-dst-port, flow-label, protocol, src-ip, l4-src-port, src-interface, src-mac, dst-mac, vlan
Other L2 packets	dst-mac, src-mac, src-interface
Other L3 (IPv4/IPv6) packets	dst-ip, src-ip, src-interface

Note

- The HASH KEY of L2 known unicast packet can support combination of one or more HASH KEYs.
- The HASH KEY of L3 known unicast packet can support combination of one or more HASH KEYs.
- The HASH KEY values of other L2 packets are fixed, and cannot be configured, fixed to use dst-mac, src-mac, src-interface to perform the load balance.
- The HASH KEY values of other L3 (IPv4/IPv6) packets are fixed, and cannot be configured, fixed to use dst-mac, src-mac, src-interface, l4-src-port and l4-dst-port to perform the load balance.

4.1.2.3 Load Balance Profile

Load balance profile is a concept of "User-Profile" specially introduced to shield chip differences among different chip manufacturers. Among them, "User" refers to all businesses that need to use the load balance of the chip (i.e. business modules, such as aggregation LAC); "Profile" is a reusable HASH configuration scheme that abstracts the underlying HASH resources.

Load balance profiles are distinguished by profile names, which are no longer than 31 characters in length. By default, there will be a default HASH profile named "default", “ecmp_default”. In addition, according to the current operating mode (single machine, stacking mode) and chip resources, users may also be provided with customizable profiles. Each profile is usually composed of the HASH KEY configuration of the L2 packet and the HASH KEY configuration of the L3 packet.

Users can flexibly configure the load balance profile and the HASH KEY of the

profile according to actual needs. After the configuration is completed, reference or bind the corresponding profile to achieve the load balance of traffic according to the corresponding profile configuration.

Note

- The name length of the load balance profile does not exceed 31 characters.
- The default name of the load balance profile is “default” “ecmp_default”, which cannot be modified.
- The default load balance profile “default” “ecmp_default” cannot be deleted, but can be configured.

4.1.3 Load Balance Profile Function Configuration

Table 220 Load balance profile function configuration list

Configuration tasks	
Load balance profile configuration function	Create one load balance profile, and enter the profile configuration mode
	Configure HASH KEY of the load balance profile
	Delete the load balance profile

4.1.3.1 Create One Load Balance Profile

After creating a load balance profile successfully, enter the corresponding load balance profile configuration mode.

Note

- The standalone user can create one customized profile at most. The stack user cannot create customized profile.

Configuration Conditions

None

Create one Load Balance Profile

Table 221 Create one load balance profile

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one load balance profile	load-balance profile { *profile-name* | default |ecmp_default}	Mandatory

Note

- By default, the system already creates the “default” “ecmp_default” profile, and the user can directly enter the configuration mode of the “default” “ecmp_default” profile via the command of creating one profile.
- The name of the created profile only supports English, and the length cannot exceed 31 characters.

4.1.3.2 Configure HASH KEY of Load Balance Profile

After creating one load balance profile successfully and entering the profile configuration mode, you can configure the HASH KEY value of the load balance profile.

Note

- The default profile of the system “default” will be configured with a default HASHKEY, and users can also modify its configuration according to actual needs.
- The default configuration of the “default” “ecmp_default” profile is: L2:src-mac, dst-mac; Ip:src-ip, dst-ip; l4-src-port, l4-dst-port.

Caution

- After creating one user customized profile, the new profile is not configured with any HASH KEY value by default, and the user needs to configure HASH KEY correctly so that the profile can be bound by the service.

Configuration Conditions

None

Configure HASH KEY of Load Balance Profile

Table 222 Configure HASH KEY of the load balance profile

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the load balance profile configuration mode	load-balance profile { *profile-name* | default|ecmp_default }	Mandatory The same as the command of creating one load balance profile
Configure HASH KEY used by L2 known unicast packet load	l2 { [dst-mac] [src-mac] [src-interface] [vlan] }	Mandatory You can configure one or more HASH KEY.
Configure HASH KEY used by L3 known unicast packet load	ip { [dst-ip] [l4-src-port] [l4-dst-port] [protocol] [src-interface] [src-ip] [flow-label] [src-mac] [dst-mac] [vlan] }	Mandatory You can configure one or more HASH KEY.
Activate the current HASH KEY configuration	active configuration pending	Mandatory
Cancel the current HASH KEY configuration	abort configuration pending	Mandatory

Note

- The HASH KEY value configured by the l2 or ip command is in the pending state, and will not take effect immediately. It can take effect only after you execute the command **active configuration pending**.
- The HASH KEY value configured by the l2 or ip command is in the pending state, and will not take effect immediately. The user can cancel the current configuration via the command **abort configuration pending**.
- When configuring new HASH KEY, it will not cover the original HASH KEY. After activating via the command **active**, the result is the communication of the original HASH KEY and the new HASH KEY.
- When the HASH KEY in the pending state is cancelled via the abort command, it will modify the original HASH KEY.
- When failed to activate, it will clear the HASH KEY in the pending state. Usually, the activating failure is because the configured HASH KEY does not meet the requirement.
- You can configure any HASH KEY for the load balance profile customized by the user. However, when used by service binding, L2 and L3 of the bound profile are required to have at least one effective HASH KEY.
- "default" and "ecmp_default" templates require that at least one hash key be configured for both L2 and L3 hash keys.

4.1.3.3 Configure HASHKEY Shift Selection of Load Balancing Profile

In the global mode, configure the shift selection of the hash key value of the corresponding load balancing profile.

Configuration Conditions

Global mode

Configure HASH KEY of Load Balancing Profile

Table 223 Configure the HASH KEY shift selection of the load balancing profile

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the HASH KEY shift selection	load-balance hash-control shift{src-mac | dst-mac|src-ip|dst-ip|vlan|l4-src-port|l4-dst-port|src-interface| flow-label| protocol } 0~5	-

4.1.3.4 Delete Load Balance Profile

The command is used to delete the load balance profile.

Note

- The default created “default” “ecmp_default” profile of the system cannot be deleted.
- The profile bound or referenced by the service cannot be deleted. To delete it, you need to remove all referencing and binding relations first.
- The un-existing profile cannot be deleted.

Configuration Conditions

None

Delete Load Balance Profile

Table 224 Delete the load balance profile

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the load balance profile configuration mode	no load-balance profile { *profile-name* }	Mandatory

4.1.4 Link Aggregation Function Configuration

Table 225 Link Aggregation Function List

Configuration Tasks	
Configure an aggregation group.	Create an aggregation group.
	Add ports into the aggregation group.
Configure the aggregation group to reference the load balance profile	Configure the aggregation group to reference the load balance profile
Configure LACP priorities.	Configure the system LACP priority.
	Configure the port LACP priority.
Configure the LACP system MAC address of the aggregation group	Configure the LACP system MAC address of the aggregation group
Configure the port ID extension of the aggregation group	Configure the port ID extension of the aggregation group
Configure the aggregation group port rate to be selected first	Configure the aggregation group port rate to be selected first
Configure the hot-swap to fast switch the root port	Configure the hot-swap to fast switch the root port

4.1.4.1 Configure an Aggregation Group

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 maximum of eight ports can join in one aggregation group at the same time.

Configuration Condition

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 226 Creating an Aggregation Group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an aggregation group.	link-aggregation *link-aggregation-id* mode { manual | lacp }	Mandatory. By default, no aggregation group is created.
Batch create aggregation groups	link-aggregation *link-aggregation-id-list* mode { manual | lacp }	Optional By default, do not create the specified aggregation group.
Enter the aggregation group configuration mode.	interface 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.
Configure the peer description information of the aggregation group	peer-description *description-name*	Optional By default, the aggregation group does not have the peer description information.

Caution

- 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 LACPDU 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 LACPDU 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 spanning tree 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 227 Adding a Port into the Aggregation Group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	-
Add the port into the	link-aggregation *link-*	By default, a port is not added

Step	Command	Description
aggregation group.	*aggregation-id* { manual | active | passive }	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, 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.
- The port configured as serviceloop-group cannot be added to the aggregation group.

4.1.4.2 Configure the Aggregation Group to Reference Load Balance Profile

By configuring the aggregation group to reference the load balance profile, you can achieve load balancing of service traffic in the aggregation group in a flexible manner.

Configuration Condition

None

Configure the Aggregation Group to Reference the Load Balance Profile

Table 228 Configuring the Aggregation Group to Reference the Load Balance Profile

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the aggregation group to reference the load balance mode	load-balance profile *profile-name*	Mandatory By default, the aggregation group references the default profile to realize the aggregation load balance.

4.1.4.3 Configure LACP Priorities

Configuration Condition

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 229 Configuring the System LACP Priority

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the system LACP priority.	lacp system-priority *system-priority-value*	Mandatory. 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 230 Configuring the Port LACP Priority

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 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.

4.1.4.4 Configure LACP System MAC Address of Aggregation Group

Configure the LACP system MAC address of the aggregation group. When the LACP system priorities at both ends of the aggregation group are the same, the smaller the LACP system MAC address, the smaller the LACP system ID (the higher the priority).

Table 231 Configure the LACP system MAC address of the aggregation group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the LACP system MAC address of the aggregation group	lacp system-mac *mac-address*	Optional By default, the LACP system MAC address of the aggregation group is the bridge MAC address of the device.

4.1.4.5 Configure Port ID Extension of Aggregation Group

If the port ID extension of the aggregation group is configured, the port number of each member port of the aggregation group in the LACP protocol is increased by 32768. This function is usually used in de stacking scenarios to avoid port ID conflicts.

Table 232 Configure the port ID extension of the aggregation group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the port ID extension of the aggregation group	lacp port-id extend	Optional By default, do not configure the port ID extension of the aggregation group.

4.1.4.6 Configure Port Rate of Aggregation Group to Be Selected First

By default, the aggregation group may select the port with low rate as the reference port. By configuring this function, the user can preferentially select the port with high rate as the reference port. After configuring this function, the aggregation group will select the reference port according to the priority of system ID - > port priority - > port rate - > port number.

Table 233 Configure the port rate of the aggregation group to be selected first

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the port rate of the aggregation group to be	lacp select speed	Optional By default, do not configure the

Step	Command	Description
selected first		port rate of the aggregation group to be selected first.

4.1.4.7 Configure Delay Forwarding Function of Aggregation Group Member Port

Configure the delay forwarding function of the aggregation group member port. The aggregation group member port on a newly inserted board or newly added device will delay for a certain time to load traffic.

Table 234 Configure the delay forwarding function of the aggregation group member port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the delay forwarding function of the aggregation group member port	lacp delay-forward *time*	Mandatory By default, the function is enabled and the delay time is 150s.

4.1.4.8 Configure Hot-swap to Fast Switch Root Port

When configuring hot-swap to fast switch the root port, we can hot-swap the card of the root port, fast inform the peer to re-select the root port, convenient for the aggregation group to converge fast.

Note

- When pulling out the card of the root port, send the fast switching notice.
- The static aggregation group does not send the fast switching notice.

Configuration Condition

None

Configure Hot-swap to Fast Switch Root Port

Table 235 Configure hot-swap to fast switch the root port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure hot-swap to fast switch the root port	link-aggregation hotswap fast-change-rootport	Mandatory By default, do not configure the hot-swap to fast switch the root port.

4.1.4.9 Link Aggregation Monitoring and Maintaining

Table 236 Link Aggregation Monitoring and Maintaining

Command	Description
show link-aggregation group [*link-aggregation-id*]	Display brief information about a specified aggregation group or all existing aggregation groups.
show link-aggregation interface [*interface-name*]	Display the details of a specified member port of an aggregation group or details of all member ports of the aggregation group.
snmp-server enable traps lacp port-status	Open the switch of the aggregation group port status change
no snmp-server enable traps lacp port-status	Close the switch of the aggregation group port status change

4.1.5 Typical Configuration Example of Link Aggregation

4.1.5.1 Configure a Static Aggregation Group

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

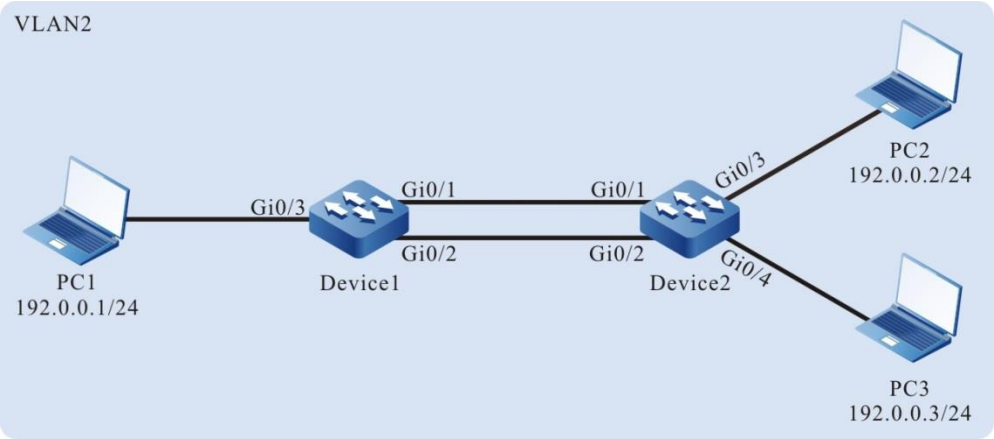


Figure 47 Networking for Configuring a Static Aggregation Group

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 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 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
  Type: switchport
  Mode: Manual
  User: LAC
  Description:
  Peer-description:
  Load balance profile: default
  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 on Device1 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 rhe aggregation group to reference the load balance profile.

#On Device1, create the load balance profile linkagg-profile.

```
Device1(config)#load-balance profile linkagg-profile
```

#On Device1, configure the packet load hash-key in the load balance profile

linkagg-profile, configure the L2 packet to load by the destination MAC, and configure the IP packet to load by the destination IP.

```
Device1(config-hashprofile)#l2 dst-mac
Device1(config-hashprofile)#ip dst-ip
Device1(config-hashprofile)#active configuration pending
```

#On Device1, configure the load balance profile referenced by aggregation group 1 as linkagg-profile.

```
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#load-balance profile linkagg-profile
```

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)#interface 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 interface link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Peer-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, view the current effective load balancing profile of aggregation group1.

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Type: switchport
  Mode: Manual
  User: LAC
  Description:
  Peer-description :
  Load balance profile: linkagg-profile
  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 balance profile of aggregation group 1 is linkagg-profile.

#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.

4.1.5.2 Configure a Dynamic Aggregation Group

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

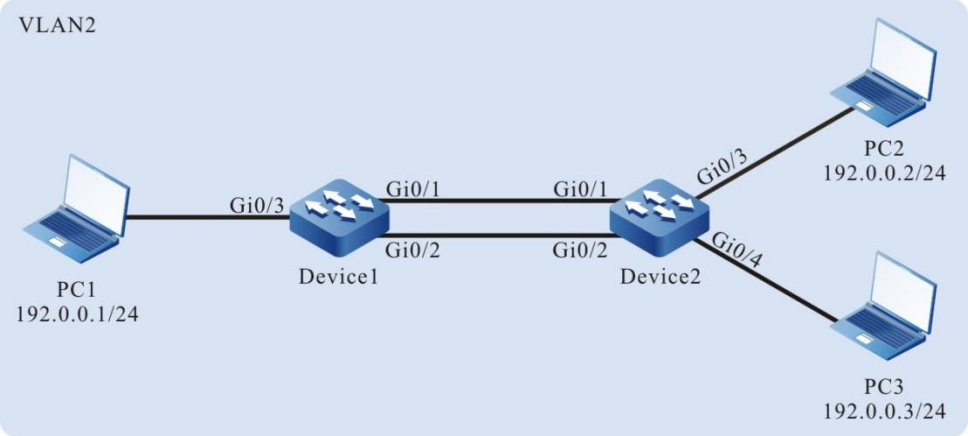


Figure 48 Networking for Configuring a Dynamic Aggregation Group

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 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 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
  Type: switchport
  Mode: LACP
  User: LAC
  Description:
  Peer-description:
  Load balance profile: default
  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 on Device1 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 aggregation group to reference the load balance profile.

#On Device1, create the load balance profile linkagg-profile.

```
Device1(config)#load-balance profile linkagg-profile
```

#On Device1, configure the packet load hash-key in the load balance profile linkagg-profile, configure the L2 packet to load by the destination MAC, configure the IP packet to load by the destination IP.

```
Device1(config-hashprofile)#l2 dst-mac
Device1(config-hashprofile)#ip dst-ip
Device1(config-hashprofile)#active configuration pending
```

#On Device1, configure the load balance profile referenced by aggregation group 1 as linkagg-profile.

```
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#load-balance profile linkagg-profile
```

On Device2, create the load balance profile linkagg-profile (omitted).

#On Device2, configure the load hash-key of the packet in the load balance profile linkagg-profile, configure the L2 packet to load by the destination MAC, configure the IP packet to load by the destination IP. (Omitted)

#On Device2, configure the load balance profile referenced by aggregation group 1 as linkagg-profile. (Omitted)

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)#interface 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.

Take Device1 for example:

```
Device1#show interface link-aggregation 1
link-aggregation 1 configuration information
    Description     :
    Peer-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 configuration, view the configured load balance profile on Device1.

```
Device1#show load-balance configuration
 Profile:default
      Configuration Valid currently:
           L2: src-mac dst-mac
           Ip: src-ip dst-ip
      Configuration Valid-pending to be applied:
           L2:
           Ip:
      Configuration Invalid-pending to be applied:
           L2:
           Ip:
Profile:linkagg-profile
      Configuration Valid currently:
           L2: dst-mac
           Ip: dst-ip
      Configuration Valid-pending to be applied:
           L2:
           Ip:
      Configuration Invalid-pending to be applied:
           L2:
           Ip:
```

#After the configuration is completed, check the current load balancing profile on Device1.

```
Device1#show link-aggregation group 1
 Link Aggregation 1
  Type: switchport
  Mode: LACP
  User: LAC
  Description:
  Peer-description :
  Load balance profile: linkagg-profile
  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 profile referenced by aggregation group 1 is linkagg-profile.

#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.

4.2 Port Isolation

4.2.1 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.

4.2.2 Port Isolation Function Configuration

Table 237 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.

4.2.2.1 Configure Basic Functions of Port Isolation

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.

Port isolation is configured based on the isolation group.

- The ports in one isolation group are isolated from each other.

The ports in the isolation group can be configured as ingress, egress, both mode, and the resolutions are as follows:

Table 238 Configuration mode forwarding table

Packet Ingress Port Mode	Packet Egress Port Mode	Forward Normally or Not
Ingress mode	ingress mode	Forward normally
ingress mode	egress mode	Forbid forwarding
ingress mode	both mode	Forbid forwarding
egress mode	ingress mode	Forward normally
egress mode	egress mode	Forward normally
egress mode	both mode	Forward normally
both mode	ingress mode	Forward normally
both mode	egress mode	Forbid forwarding
both mode	both mode	Forbid forwarding

- The ports in the isolation group communicate with the ports not added to the isolation group normally.

The ports of different isolation groups can communicate normally.

Configuration Condition

The isolation group is already created.

Configure Port Isolation

Table 239 Configuring Port Isolation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the isolation group	isolate group *group-id*	Mandatory

Step	Command	Description
configuration mode		
Add the port to the isolation group	interface link-aggregation *link-aggregation-id* [ingress | egress | both]	Mandatory By default, the port is not added to the isolation group.
Add the aggregation group to the isolation group	link-aggregation *link-aggregation-id* [ingress | egress | both]	Mandatory By default, the aggregation group is not added to the isolation group.

Note

- When adding one port to the isolation group, the isolation group needs to be created.

4.2.2.2 Port Isolation Monitoring and Maintaining

Table 240 Port Isolation Monitoring and Maintenance

Command	Description
show isolate { group [*group-id*] | interface *interface-list* | interface link-aggregation *link-aggregation-id* }	Displays the port isolation information.

4.2.3 Typical Configuration Example of Port Isolation

4.2.3.1 Configure Port Isolation

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

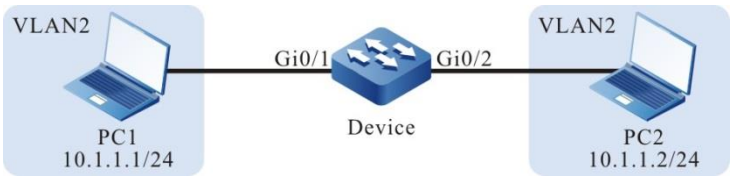


Figure 49 Networking for Configuring Port Isolation

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 the isolation group.

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group1)#
Device(config-isolate-group1)#end
Device#show isolate group 1
------------------------------------------------------------
isolate group 1
ingress member:
egress member :
both member   :
```

#On Device, configure port isolation between port gigabitethernet0/1 and port gigabitethernet0/2.

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group1)#interface gigabitethernet 0/1-0/2
```

```
Device#show isolate group 1
------------------------------------------------------
            isolate group 1
ingress member:
egress member :
both members  : gi0/1-0/2
```

#On Device, query the port isolation information.

```
Device#show isolate interface gigabitethernet 0/1-0/2
interface gigabitethernet0/1 isolated information
 isolate group 1 mode: both
 isolated interface:
          gi0/2
interface gigabitethernet0/2 isolated information
 isolate group 1 mode: both
 isolated interface:
          gi0/1
```

Step 3: Check the result.

#PC1 and PC2 cannot communicate with each other.

4.3 VLAN

4.3.1 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 Local Area Network (LAN) can receive the packets. This not only wastes network bandwidth, but also brings hidden troubles.

Virtual Local Area Network (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.

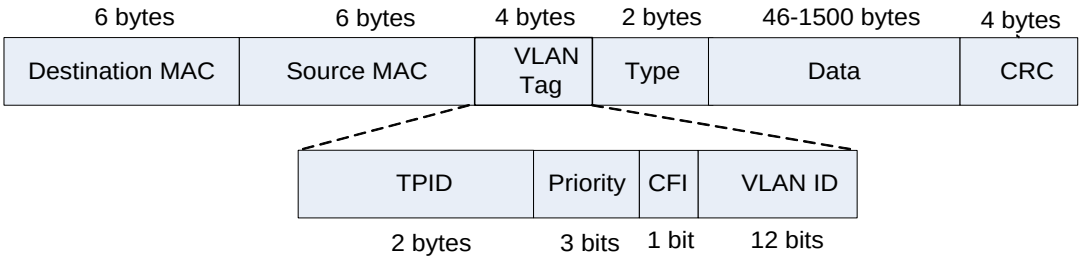


Figure 50 IEEE 802.1Q Frame Encapsulation Format

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: IP subnet-based VLANs, MAC-based VLANs, protocol-based VLANs, and port-based VLANs. On one port, the VLANs take effect according to the priority levels, and only one type of VLAN takes effect.

4.3.2 VLAN Function Configuration

Table 241 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.

4.3.2.1 Configure Basic Attributes of VLANs

Configuration Condition

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 242 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 243 Configure the VLAN name.

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enters the VLAN configuration	vlan *vlan-id*	-

Step	Command	Description
mode.		
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.

4.3.2.2 Configure a Port-Based VLAN

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 Condition

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 244 Configuring the Port Link Type

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.	interface link-aggregation *link-aggregation-id*	
Configure the port link type.	switchport mode { access | hybrid | trunk }	Mandatory. By default, the port link type is the Access type.

Caution

- 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 245 Adding an Access Port into the VLAN

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.	interface link-aggregation *link-aggregation-id*	
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 246 Configuring a Trunk Port to Allow Services of a VLAN to Pass

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.	interface 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.
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 247 Adding a Hybrid Port into the VLAN

Step	Command	Description
Enter the 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 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.	interface 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. 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 248 Configuring PVIDs for Ports

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.	interface 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.

4.3.2.3 Configure a MAC Address-Based VLAN

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.

Configuration Condition

None

Configure a MAC Address-Based VLAN

Table 249 Configuring a MAC Address-Based VLAN

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure a MAC VLAN entry.	mac-vlan mac-address *mac-address* vlan *vlan-id*	Mandatory. By default, no MAC VLAN entry is configured.
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.	interface link-aggregation *link-aggregation-id*	
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.

4.3.2.4 Configure an IP Subnet-Based VLAN

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.

Configuration Condition

None

Configure an IP Subnet-Based VLAN

Table 250 Configuring an IP Subnet-Based VLAN

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*	Mandatory. By default, no IP subnet VLAN entry is configured.
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After entering the L2 Ethernet interface configuration mode, the subsequent configuration
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		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 IP subnet VLAN function of the port.	ip-subnet-vlan enable	Mandatory. By default, the IP subnet VLAN function is disabled on the port.

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.

4.3.2.5 Configure a Protocol-Based VLAN

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.

Configuration Condition

None

Configure a Protocol-Based VLAN

Table 251 Configuring a Protocol-Based VLAN

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 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.	interface link-aggregation *link-aggregation-id*	
Configure the matching protocol profile of the port	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.

4.3.2.6 Configure the Types of Frames that Can Be Received by the Port

Configuration Condition

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 252 Configuring the Types of Frames that Can Be Received by the Port

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.	interface link-aggregation *link-aggregation-id*	
Configure the types of frames that can be received by the	switchport accept frame-type { all | untag | tag }	Mandatory. By default, the type of frames

Step	Command	Description
port.		that can be received by a port is all, that is, receiving both Untag and Tag packets.

4.3.2.7 VLAN Monitoring and Maintaining

Table 253 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 vlan summary	Displays the static created and dynamic learned VLAN information
show { interface *interface-name* | interface link-aggregation *link-aggregation-id* } vlan status	Displays the VLAN information on the specified port or aggregation group.

4.3.3 VLAN Typical Configuration Example

4.3.3.1 Configure Port-Based VLANs

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

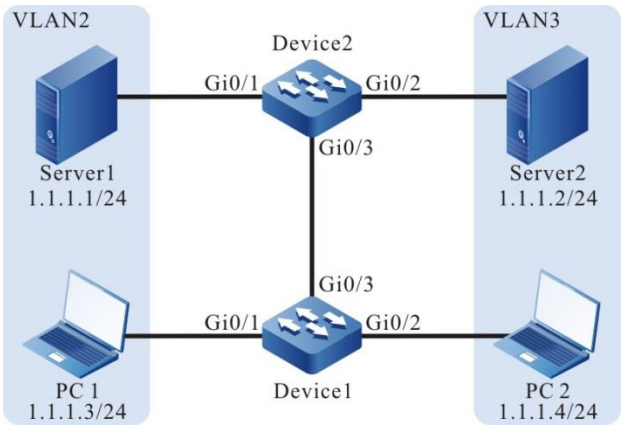


Figure 51 Networking for Configuring Port-Based VLANs

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 trunk 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.

4.3.3.2 Configure MAC Address-Based VLANs

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

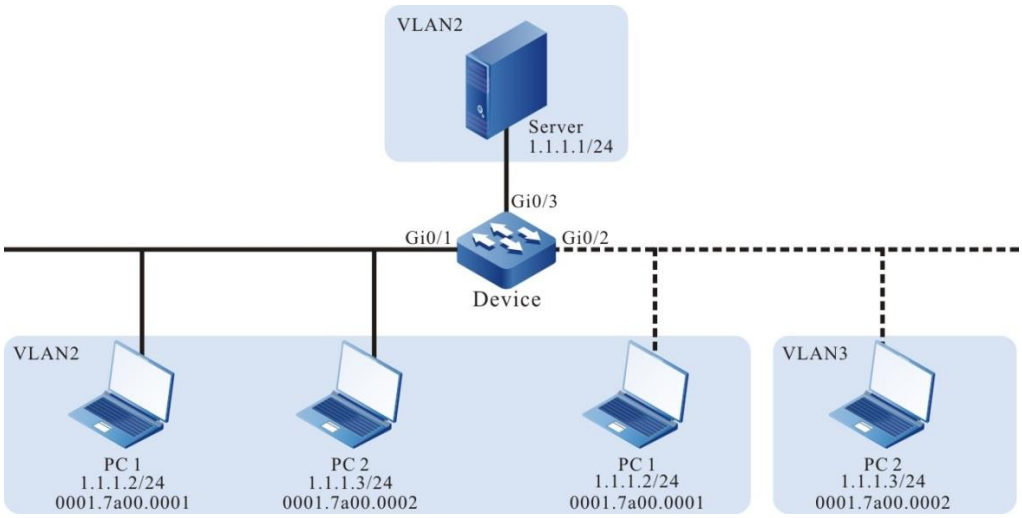


Figure 52 Networking for Configuring MAC address-Based VLANs

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 0101.7a00.0001 can be forwarded in VLAN2.

```
Device(config)#mac-vlan mac-address 0101.7a00.0001 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 512,    used 1,    left 511

--------------------------------MAC-VLAN---------------------------------
NO.   Mac Address     Dynamic Vlan  Static Vlan  Current Pri  Static Pri
----- --------------- ------------ ------------ ------------ -----------
1     0101.7a00.0001  0          2          -          -

-----------------------------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.

4.3.3.3 Configure IP Subnet-Based VLANs

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

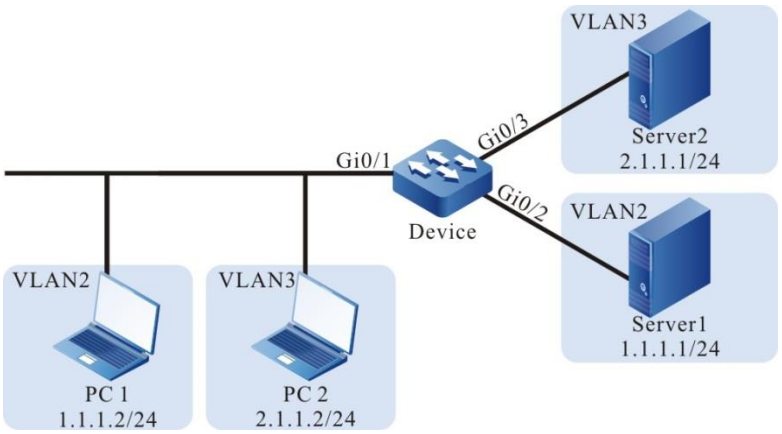


Figure 53 Configuring an IP Subnet-Based VLAN

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      -

----------------------Enable SUBNET-VLAN----------------------
gi0/1

------------------Enable SUBNET-VLAN Priority------------------
#PC1 can access only Server1 and PC2 can access only Server2.
```

4.3.3.4 Configure Protocol-Based VLANs

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

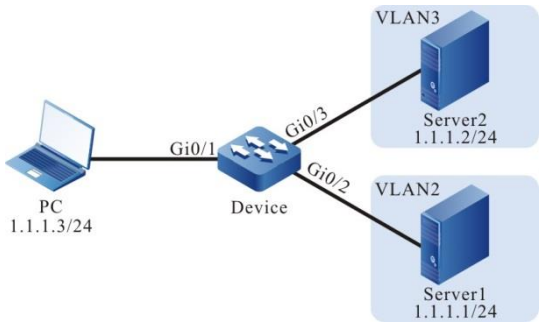


Figure 54 Networking for Configuring Protocol-Based VLANs

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 enable
Device(config-if-gigabitethernet0/1)#protocol-vlan profile 1 vlan 3
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

---------------------------PROTOTOCL-VLAN-------------------------
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
```

#When the protocol-based VLAN function is not 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.

4.4 QinQ and VLAN Mapping

4.4.1 Overview

802.1Q in 802.1Q (QinQ), which is an extension of the 802.1Q protocol, adds a layer of 802.1Q tag (VLAN tag) on the basis of the original 802.1Q packet header. By

use of two layers of VLAN tags, the number of VLANs is increased to 4094x4094. QinQ encapsulates user private network VLAN tags into public network VLAN tags so that the packets are transmitted in the carrier backbone network (public network) with two layers of VLAN tags. In the public network, the packets are broadcasted based on the outer VLAN tags (that is, public network VLAN tags), and the user private network VLAN tags are shielded. This saves public network VLAN IDs, and provides a simple L2 Virtual Private Network (VPN) tunnels for users.

According to rules of adding VLAN tags, QinQ falls into the following types:

- Basic QinQ
- Port-based flexible QinQ

VLAN mapping is also an extension of 802.1Q. It is different from QinQ in the following aspect: Instead of encapsulating another layer of VLAN tag on the basis of the original VLAN tag of a packet, VLAN mapping replaces the original VLAN tag of a packet with a new VLAN tag. In this way, the packet still has only one layer of VLAN tag.

According to the mapping rules, VLAN mapping falls into the following types:

- 1:1 VLAN mapping. Only one private network VLAN can be mapped into one public network VLAN.
- N:1 VLAN mapping. That is, one or more private VLANs can be mapped to a public VLAN.

For port-based flexible QinQ, 1:1 VLAN mapping, private network VLAN to public network VLAN mapping entries must be configured. A user can configure a maximum of 4096 mapping entries.

4.4.2 QinQ and VLAN Mapping Function Configuration

Table 254 QinQ and VLAN Mapping Function List

Configuration Tasks	
Configure the basic QinQ function.	Enable the basic QinQ function.

Configuration Tasks	
Configure the port-based flexible QinQ function.	Configure the port-based flexible QinQ function.
Configure the 1:1 VLAN mapping function.	Configure the 1:1 VLAN mapping function.
Configure the N:1 VLAN mapping function.	Configure the N:1 VLAN mapping function.
Configure the protocol type of the outer VLAN tag of a port.	Configure the protocol type of the outer VLAN tag of a port.
Configure the priority duplication function.	Enable the priority duplication function.
Configure the QinQ Drop function	Configure the QinQ Drop function

4.4.2.1 Configure the Basic QinQ Function

After the basic QinQ function is configured on a port, the device adds another layer of VLAN tags for the packets received from the port. The VLAN ID of the VLAN tags is the PVID of the port.

Configuration Condition

Before configuring the basic QinQ function, ensure that:

- The PVID of the port has been configured. The PVID is the VLAN ID of the outer VLAN tags that are added to packets after the basic QinQ function of the port is enabled.

Enable the Basic QinQ Function

Table 255 Enabling the Basic QinQ Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter the L2 Ethernet interface configuration mode, the subsequent

Step	Command	Description
Enter the aggregation group configuration mode.	link-aggregation *link-aggregation-id*	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 basic QinQ function.	vlan dot1q-tunnel enable	Mandatory. By default, the basic QinQ function is disabled.

Note

- On one port, the basic QinQ function cannot coexist with the following functions: QinQ Evc, flexible QINQ, 1:1 VLAN mapping, N:1 VLAN mapping, configure the protocol type of the outer VLAN tags of the port as a non-default value.

4.4.2.2 Configure the Port-Based Flexible QinQ Function

After a port is configured with the port-based flexible QinQ, if the VLAN ID of the outermost layer of VLAN tag of a packet matches an entry of the port-based flexible QinQ, a specified outer VLAN tag is added to the packet. If the VLAN ID of the outermost layer of VLAN tag of a packet does not match an entry of the port-based flexible QinQ, a layer of VLAN tag is added to the packet, and the VLAN ID of the VLAN tag is the PVID of the port.

Configuration Condition

Before configuring the port-based flexible QinQ function, ensure that:

- The port link type is configured to the Trunk type or the Hybrid type.
- A PVID has been configured for the port.

- The VLAN of the outer VLAN tags to be added has been configured for the port, and the packets to which outer VLAN tags have been added can pass the VLAN.

Configure the Port-Based Flexible QinQ Function

Table 256 Configuring the Port-Based Flexible QinQ Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter the L2 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 port-based flexible QinQ entries.	vlan dot1q-tunnel *inner-vlan-list outer-vlan-id*	Mandatory. By default, port-based flexible QinQ entries are not configured.

Note

- On one port, the port-based flexible QinQ function cannot coexist with the following functions: QinQ Evc, basic QINQ, 1:1 VLAN mapping, N:1 VLAN mapping.
- When the configured port-based flexible QinQ entry conflicts with the

existing port-based flexible QinQ entry of the port, a conflict will be prompted.

4.4.2.3 Configure the 1:1 VLAN Mapping Function

For a port, 1:1 VLAN mapping entry is a one-to-one mapping, that is, the 1:1 VLAN mapping entry maps a private network VLAN to a public network VLAN.

After a port is configured with 1:1 VLAN mapping, if the outmost VLAN tag of a packet matches a 1:1 VLAN mapping entry, the port replaces the VLAN ID of the outmost VLAN tag with the specified VLAN ID. If the outmost VLAN tag of a packet does not match a 1:1 VLAN mapping entry, the port add a layer of VLAN tag to the packet, and the VLAN ID of the VLAN tag is the PVID of the port.

Configuration Condition

Before configuring the 1:1 VLAN mapping function, ensure that:

- The port link type is configured to the Trunk type or the Hybrid type.
- A PVID has been configured for the port.
- The VLAN of the new outer VLAN tag used for replacing the existing VLAN tag has been configured for the port, and the packets for which the outer VLAN tags have been replaced can pass the VLAN.

Configure the 1:1 VLAN Mapping Function

Table 257 Configuring the 1:1 VLAN Mapping Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter 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 you enter the aggregation group configuration mode, the subsequent configuration takes effect only within the aggregation group.
Configure 1:1 VLAN mapping function entries.	vlan dot1q-tunnel mapping *former-vlan-id mapping-vlan-id*	Mandatory. By default, 1:1 VLAN mapping entries are not configured.

Note

- On one port, the 1:1 VLAN mapping function cannot coexist with the following functions: QinQ Evc, basic QINQ, flexible QINQ, N:1 VLAN mapping.
- If the configured 1:1 VLAN mapping entry conflicts with an existing port-based 1:1 VLAN mapping entry, the conflict will be prompted.

4.4.2.4 Configure the N: 1 VLAN Mapping Function

For a port, multiple N:1 VLAN mapping entries can be configured. Each N:1 VLAN mapping entry can be the multiple-to-one relationship, that is, one or more private VLANs can be mapped to a public VLAN.

After the port is configured with N: 1 VLAN mapping, if the VLAN ID of the outermost VLAN tag of the packet matches the entry of N: 1 VLAN mapping, replace the VLAN ID of the outermost VLAN tag of the packet with the specified VLAN ID; if not, the N: 1 VLAN mapping will not process the packet.

Configuration Condition

Before configuring the N:1 VLAN mapping function, ensure that:

- The port link type is configured to the Trunk type or the Hybrid type.
- Configure the port to add the VLAN of the replaced outer VLAN tag to ensure that the packet after replacing the outer VLAN tag can pass.

Configure N: 1 VLAN Mapping Function

Table 258 Configure N:1 VLAN mapping function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter the L2 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 N:1 VLAN mapping function	vlan dot1q-tunnel mapping n-to-1 enable	Mandatory By default, do not enable the N: 1 VLAN mapping function
Configure the entry of N:1 VLAN mapping	vlan dot1q-tunnel mapping n-to-1 *former-vlan-list mapping-vlan-id*	Mandatory By default, do not configure the entry of N:1 VLAN mapping.

Note

- On one port, the N:1 VLAN mapping function cannot coexist with the following functions: QinQ Evc, basic Qin Q, port-based flexible QINQ, 1:1 VLAN mapping, configure the protocol type of the outer VLAN tags of the port as a non-default value.

4.4.2.5 Configure the Protocol Type of the Outer VLAN Tag of a Port

A port determines whether a packet carries the corresponding VLAN tag based on the Tag Protocol Identifier (TPID). After a port receives a packet, it compares the TPID that is configured on the port with the corresponding field in the packet. If they are the same, it indicates that the packet carries the corresponding VLAN tag. If they are different, the device regards and handles the received packet as an Untag packet.

Devices of some manufacturers may set the TPID field of outer VLAN tags of QinQ packets to 0x9100 or other values. To be compatible with the devices, the TPID value of the outer VLAN tags of the local device port must be configured to the same value.

Configuration Condition

None

Configure the Protocol Type of the Outer VLAN Tag of a Port

A device supports three TPID values. The value range of TPIDs is 0x0001-0xffff, and it cannot be the reserved protocol field such as 0x0806 and 0x0800.

Table 259 Configuring the Protocol Type of the Outer VLAN Tag of a Port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet	interface *interface-name*	Either

Step	Command	Description
interface configuration mode.		After you enter the L2 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 protocol type of the outer VLAN tag of a port.	frame-tag tpid *type-value*	Optional. By default, the protocol type value of outer VLAN tags of a port is 0x8100.

Note

- On one port, configure the protocol type of the port outer VLAN tag as the non-default value, which cannot coexist with the following functions: QinQ Evc, basic Qin Q, flexible QINQ, 1:1 VLAN mapping, N:1 VLAN mapping.

4.4.2.6 Configure the Priority Duplication Function

After a port is configured with the priority duplication function, it duplicates the priority field of the outmost VLAN tag of an original packet to the priority field of the outmost VLAN tag of the packet.

Configuration Condition

To configure the priority duplication function, first complete the following task:

- Configure the basic QinQ function and the port-based flexible QinQ function

or 1:1 VLAN mapping function.

Enable the Priority Duplication Function

Table 260 Enabling the Priority Duplication Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter the L2 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 priority duplication function	inner-priority-trust enable	Mandatory. By default, the priority duplication function is disabled.

4.4.2.7 Configure QinQ Drop Function

After the port is configured with the QinQ drop function, if the port receives a packet that does not match the port-based flexible QinQ entry, 1:1 VLAN mapping entry and N:1 VLAN mapping entry, the packet will be discarded.

Configuration Condition

To configure the QinQ Drop function, first complete the following task:

- Configure the basic QinQ function and the port-based flexible QinQ function or 1:1 VLAN mapping function.

Enable QinQ Drop Function

Table 261 Enable QinQ Drop function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode.	interface *interface-name*	Either After you enter the L2 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 QinQ Drop function	vlan dot1q-tunnel drop	Mandatory By default, the QinQ Drop function is not enabled.

Note

- On one port, the QinQ Drop function cannot coexist with QinQ Evc.

4.4.2.8 QinQ and VLAN Mapping Monitoring and Maintaining

Table 262 QinQ and VLAN Mapping Monitoring and Maintaining

Command	Description
show vlan dot1q-tunnel	Displays the of port-based flexible QinQ configuration.
show vlan dot1q-tunnel mapping	Displays the 1:1 VLAN mapping configuration.
show vlan dot1q-tunnel mapping n-to-1 configuration	Displays the N:1 VLAN mapping configuration.

4.4.3 Typical Configuration Example of QinQ and VLAN Mapping

4.4.3.1 Configure Basic QinQ

Network Requirements

- Intranet users CE1 and CE2, and CE3 and CE4 communicate with each other through the carrier network. CE1 and CE2 uses the Intranet VLAN10-VLAN20, CE3 and CE4 uses Intranet VLAN15-VLAN30, and PE1 and PE2 are two edge devices in the carrier network.
- The basic QinQ is configured on PE1 and PE2. Then, CE1 and CE2 can communicate with each other through VLAN00 of the carrier public network, CE3 and CE4 can communicate with each other through VLAN101 of the carrier public network, and the packets that are transmitted in the carrier public network contain two layers of tags.

Network Topology

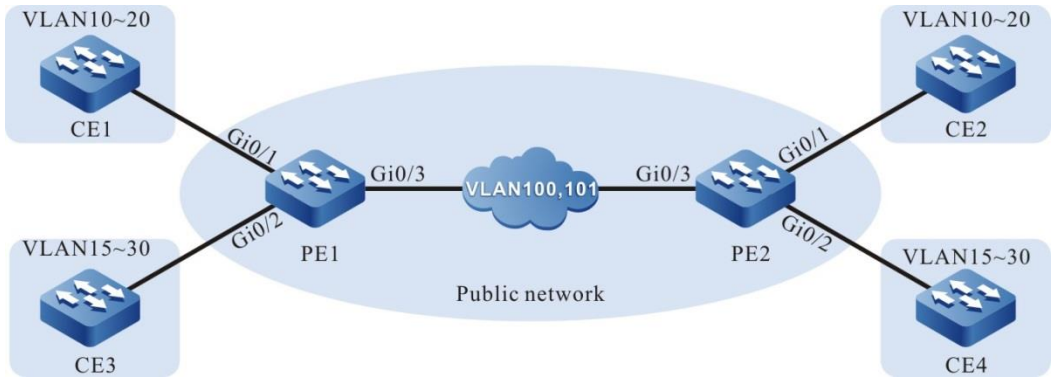


Figure 55 Networking for Configuring Basic QinQ

Configuration Steps

Step 1: Configure PE1.

#On PE1, create VLAN10-VLAN30 and VLAN100-VLAN101.

```
PE1#configure terminal
```

```
PE1(config)#vlan 10-30,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN10-VLAN20 and VLAN100 to pass, and set PVID to 100.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN15-VLAN30 and VLAN 101 to pass, and set PVID to 101.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE1(config)#interface gigabitethernet0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#On ports gigabitethernet0/1 and gigabitethernet0/2 of PE1, enable the basic QinQ function.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/1)#exit
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure PE2.

#On PE2, create VLAN10-VLAN30 and VLAN100-VLAN101.

```
PE2#configure terminal
PE2(config)#vlan 10-30,100-101
```

#On PE2, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN10-VLAN20 and VLAN100 to pass, and set PVID to 100.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#switchport mode trunk
PE2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE2(config-if-gigabitethernet0/1)#exit
```

#On PE2, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN15-VLAN30 and VLAN 101 to pass, and set PVID to 101.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#switchport mode trunk
PE2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE2(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE2(config)#interface gigabitethernet 0/3
PE2(config-if-gigabitethernet0/3)#switchport mode trunk
PE2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/3)#exit
```

#On ports gigabitethernet0/1 and gigabitethernet0/2 of PE2, enable the basic QinQ function.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE2(config-if-gigabitethernet0/1)#exit
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE2(config-if-gigabitethernet0/2)#exit
```

Step 3: Check the result.

#Through PE1 and PE2, the services of Intranet users CE1 and CE2 can be transmitted in VLAN100 of the carrier network with two layers of tags. Through PE1 and PE2, the services of Intranet users CE3 and CE4 can be transmitted in VLAN101 of the carrier network with two layers of tags.

4.4.3.2 Configure Flexible QinQ

Network Requirements

- Intranet users CE1 and CE2, and CE3 and CE4 communicate with each other through the carrier network. CE1 and CE2 uses the Intranet VLAN10-VLAN20, CE3 and CE4 uses Intranet VLAN15-VLAN30, and PE1 and PE2 are two edge devices in the carrier network.
- Flexible QinQ is configured on PE1 and PE2. Then, CE1 and CE2 can communicate with each other through VLAN00 of the carrier public network, CE3 and CE4 can communicate with each other through VLAN101 of the carrier public network, and the packets that are transmitted in the carrier public network contain two layers of tags.

Network Topology

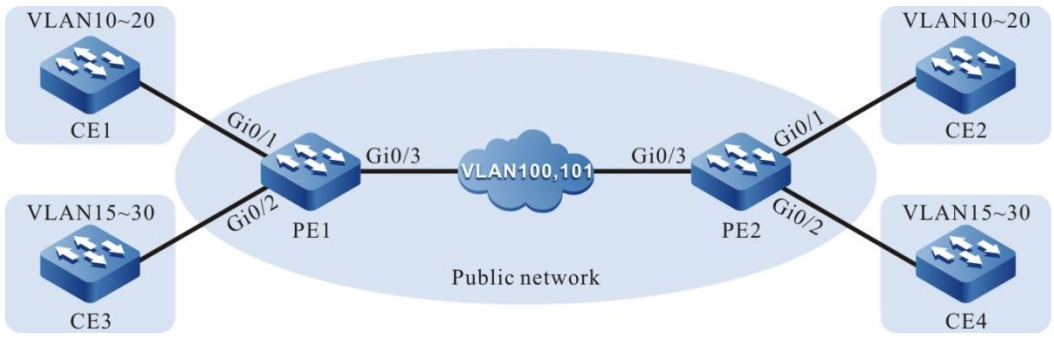


Figure 56 Networking for Configuring Flexible QinQ

Configuration Steps

Step 1: Configure PE1.

#On PE1, create VLAN10-VLAN30 and VLAN100-VLAN101.

```
PE1#configure terminal
PE1(config)#vlan 10-30,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN10-VLAN20 and VLAN100 to pass, and set PVID to 100.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN15-VLAN30 and VLAN 1 to pass, and set PVID to 101.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE1(config)#interface gigabitethernet 0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#On port gigabitethernet0/1 of PE1, configure the flexible QinQ function so that VLAN tags of VLAN100 are added to the packets of VLAN10-VLAN20.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel 10-20 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On port gigabitethernet0/2 of PE1, configure the flexible QinQ function so that VLAN tags of VLAN101 are added to the packets of VLAN15-VLAN30.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel 15-30 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, query the information about flexible QinQ entries.

```
PE1#show vlan dot1q-tunnel
------------------------------------ ------------VLAN DOT1Q-TUNNEL------------ ---
--------------------------------
Interface          priority-default   Inner VlanId   Outer VlanId   inner-priority-trust   Inner
VlanId Count
------------------  ----------------  ------------  ------------  ------------------
--  -----------------
gi0/1              disable           10-20          100           /                11
gi0/2              disable           15-30          101           /                16
```

Step 2: Configure PE2.

#On PE2, create VLAN10-VLAN30 and VLAN100-VLAN101.

```
PE2#configure terminal
PE2(config)#vlan 10-30,100-101
```

#On PE2, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN10-VLAN20 and VLAN100 to pass, and set PVID to 100.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#switchport mode trunk
PE2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 10-20,100
PE2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 100
PE2(config-if-gigabitethernet0/1)#exit
```

#On PE2, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN15-VLAN30 and VLAN 1 to pass, and set PVID to 101.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#switchport mode trunk
PE2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 15-30,101
PE2(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 101
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE2(config)#interface gigabitethernet 0/3
PE2(config-if-gigabitethernet0/3)#switchport mode trunk
PE2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/3)#exit
```

#On port gigabitethernet0/1 of PE2, configure the flexible QinQ function so that VLAN tags of VLAN100 are added to the packets of VLAN10-VLAN20.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel 10-20 100
PE2(config-if-gigabitethernet0/1)#exit
```

#On port gigabitethernet0/2 of PE2, configure the flexible QinQ function so that VLAN tags of VLAN101 are added to the packets of VLAN15-VLA30.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
```

```
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel 15-30 101
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, query the information about flexible QinQ entries.

```
PE2#show vlan dot1q-tunnel
---------------------------------- ------------VLAN DOT1Q-TUNNEL------------ ---
--------------------------------
Interface          priority-default   Inner VlanId   Outer VlanId   inner-priority-trust   Inner
VlanId Count
------------------  ----------------  ------------  ------------  ------------------
--  -----------------
gi0/1              disable           10-20         100           /                11
gi0/2              disable           15-30         101           /                16
```

Step 3: Check the result.

#Through PE1 and PE2, the services of Intranet users CE1 and CE2 can be transmitted in VLAN100 of the carrier network with two layers of tags. Through PE1 and PE2, the services of Intranet users CE3 and CE4 can be transmitted in VLAN101 of the carrier network with two layers of tags.

4.4.3.3 Configure the 1:1 VLAN Mapping

Network Requirements

- Intranet users CE1 and CE2, and CE3 and CE4 communicate with each other through the carrier network. CE1 and CE2 uses the Intranet VLAN2, CE3 and CE4 uses Intranet VLAN3, and PE1 and PE2 are two edge devices in the carrier network.
- 1:1 VLAN mapping is configured on PE1 and PE2. Then, CE1 and CE2 can communicate with each other through VLAN00 of the carrier public network, CE3 and CE4 can communicate with each other through VLAN101 of the carrier public network, and the packets that are transmitted in the carrier public network contain two layers of tags.

Network Topology

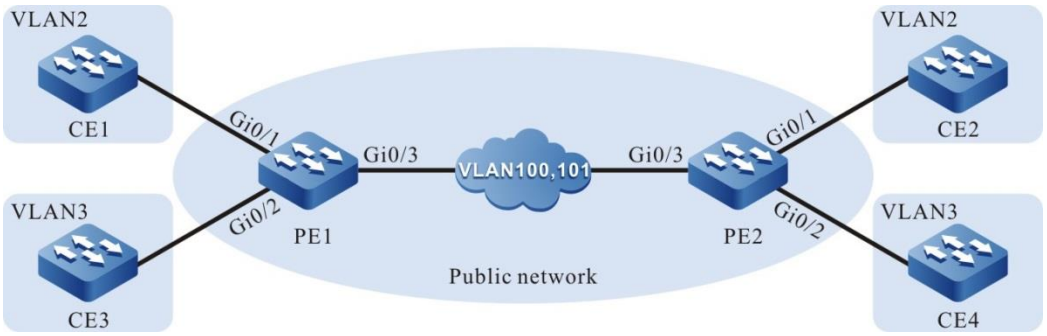


Figure 57 Configuring 1:1 VLAN Mapping

Configuration Steps

Step 1: Configure PE1.

#On PE1, create VLAN2-VLAN3 and VLAN100-VLAN101.

```
PE1#configure terminal
PE1(config)#vlan 2-3,100-101
```

#On PE1, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2 and VLAN100 to pass, and set PVID to 1.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#switchport mode trunk
PE1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2,100
PE1(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/1)#exit
```

#On PE1, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN101 to pass, and set PVID to 1.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#switchport mode trunk
PE1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 3,101
PE1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE1(config)#interface gigabitethernet 0/3
PE1(config-if-gigabitethernet0/3)#switchport mode trunk
PE1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE1(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE1(config-if-gigabitethernet0/3)#exit
```

#On port gigabitethernet0/1 of PE1, configure the 1:1 VLAN mapping function so that the data of VLAN2 is changed to VLAN100.

```
PE1(config)#interface gigabitethernet 0/1
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping 2 100
PE1(config-if-gigabitethernet0/1)#exit
```

#On port gigabitethernet0/2 of PE1, configure the 1:1 VLAN mapping function so that the data of VLAN3 is changed to VLAN101.

```
PE1(config)#interface gigabitethernet 0/2
PE1(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE1(config-if-gigabitethernet0/2)# vlan dot1q-tunnel mapping 3 101
PE1(config-if-gigabitethernet0/2)#exit
```

#On PE1, query the information about 1:1 VLAN mapping entries.

```
PE1# show vlan dot1q-tunnel mapping
---------------------------------- -------VLAN DOT1Q-TUNNEL MAPPING------ -------
----------------------------------
Interface            priority-default    Former VlanId   Mapping VlanId  inner-priority-trust
Former VlanId Count
-------------------- -------------------- -------------- --------------- ------------
---------- --------------------
gi0/1            disable         2           100          /              1
gi0/2            disable         3           101          /              1
```

Step 2: Configure PE2.

#On PE2, create VLAN2-VLAN3 and VLAN100-VLAN101.

```
PE2#configure terminal
PE2(config)#vlan 2-3,100-101
```

#On PE2, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2 and VLAN100 to pass, and set PVID to 1.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#switchport mode trunk
PE2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2,100
PE2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/1)#exit
```

#On PE2, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN3 and VLAN101 to pass, and set PVID to 1.

```
PE2(config)#interface gigabitethernet 0/2
```

```
PE2(config-if-gigabitethernet0/2)#switchport mode trunk
PE2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 3,101
PE2(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, configure the link type of port gigabitethernet0/3 to Trunk and allow services of VLAN100 and VLAN101 to pass, and set PVID to 1.

```
PE2(config)#interface gigabitethernet 0/3
PE2(config-if-gigabitethernet0/3)#switchport mode trunk
PE2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 100,101
PE2(config-if-gigabitethernet0/3)#switchport trunk pvid vlan 1
PE2(config-if-gigabitethernet0/3)#exit
```

#On port gigabitethernet0/1 of PE2, configure the 1:1 VLAN mapping function so that the data of VLAN2 is changed to VLAN100.

```
PE2(config)#interface gigabitethernet 0/1
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel enable
PE2(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping 2 100
PE2(config-if-gigabitethernet0/1)#exit
```

#On port gigabitethernet0/2 of PE2, configure the 1:1 VLAN mapping function so that the data of VLAN3 is changed to VLAN101.

```
PE2(config)#interface gigabitethernet 0/2
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel enable
PE2(config-if-gigabitethernet0/2)#vlan dot1q-tunnel mapping 3 101
PE2(config-if-gigabitethernet0/2)#exit
```

#On PE2, query the information about 1:1 VLAN mapping entries.

```
PE2# show vlan dot1q-tunnel mapping
---------------------------------- -------VLAN DOT1Q-TUNNEL MAPPING------ -------
----------------------------------
Interface            priority-default    Former VlanId   Mapping VlanId  inner-priority-trust
Former VlanId Count
-------------------- -------------------- -------------- --------------- ------------
---------- -------------------
gi0/1            disable         2           100         /              1
gi0/2            disable         3           101         /              1
```

Step 3: Check the result.

#Through PE1 and PE2, the services of Intranet users CE1 and CE2 can be transmitted in VLAN100 of the carrier network with one layer of tags. Through PE1

and PE2, the services of Intranet users CE3 and CE4 can be transmitted in VLAN101 of the carrier network with one layer of tags.

4.4.3.4 Configure the N:1 VLAN Mapping

Network Requirements

- On device2, PC1 and PC2 are isolated from each other in different VLANs.
- Configure the N:1 VLAN mapping function on Device1 to realize the transmission of PC1 and PC2 service packets in the same VLAN when passing through Device1, so as to save VLAN resources.

Network Topology

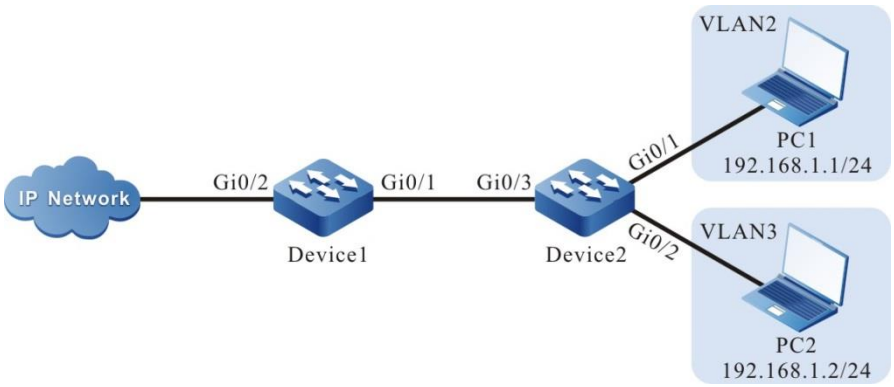


Figure 58 Configuring N:1 VLAN Mapping

Configuration Steps

Step 1: Configure Device1.

#Create VLAN2-VLAN4 on Device1.

```
Device1#configure terminal
Device1(config)#vlan 2-4
```

#On Device1, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2 and VLAN100 to pass, and set PVID to 1.

```
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)#switchport trunk pvid vlan 1
```

#Configure the N:1 VLAN mapping function on the port gigabitothernet0 / 1 of Device1 to map VLAN2 and VLAN3 to vlan4.

```
Device1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping n-to-1 enable
Device1(config-if-gigabitethernet0/1)#vlan dot1q-tunnel mapping n-to-1 2-3 4
Device1(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on Device1 as trunk, which allows vlan2 - vlan4 services to pass through, and the PVID is configured as 1.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/2)#switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/2)#exit
```

Step 2: Configure Device2.

#Create VLAN2 and VLAN3 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#On Device2, configure the link type of port gigabitethernet0/1 to Access and allow 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
```

#On Device2, configure the link type of port gigabitethernet0/1 to Access and allow services of VLAN3 to pass.

```
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
```

#On Device2, configure the link type of port gigabitethernet0/1 to Trunk and allow services of VLAN2 and VLAN3 to pass, and configure PVID to 1.

```
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)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/3)#exit
```

Step 3: Check the result.

#On Device1, query the entry information of N:1 VLAN mapping.

```
Device1# show vlan dot1q-tunnel mapping n-to-1 configuration
---- ------------------ ------- ---------------------------------- -------------
NO.  Name               Status  Customer Member                    Service VLAN
---- ------------------ ------- ---------------------------------- -------------
1    gi0/1              enable  2-3                                4
```

#On Device2, the services of PC1 and PC2 are isolated from each other, the service packets of PC1 are transmitted in VLAN2, and the service packets of PC2 are transmitted in VLAN3.

#The service packets of PC1 and PC2 accessing IP Network are forwarded through VLAN4 of Device1.

4.5 Super-VLAN

4.5.1 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)/ND 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/IPv6 address resources.

4.5.2 VLAN Function Configuration

Table 263 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

Configuration Tasks	
	super-VLAN.
Enable the ARP proxy function.	Enable the ARP proxy function.
Enable the ND proxy function	Enable the ND proxy function

4.5.2.1 Configure a Super VLAN

Configuration Condition

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 264 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.

4.5.2.2 Configure Sub-VLAN Members of a Super-VLAN

Configuration Condition

None

Configure Sub-VLAN Members of a Super-VLAN

One super-VLAN supports a maximum of 128 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 265 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.

Caution

- The configured Sub-VLAN cannot be configured as the EIPS control vlan.

4.5.2.3 Enable the ARP Proxy Function

Configuration Condition

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 266 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.

4.5.2.4 Enable the ND Proxy Function

Configuration Condition

Before enabling the ND proxy function, ensure that:

- The VLAN interface corresponding to the super-VLAN and the IPv6 address have been configured.

Configure the ND Proxy Function

After enabling the ND proxy function of Super-VLAN, IPv6 L3 interworking can be realized between Sub-VLAN through ND proxy.

Table 267 Enable the ND proxy function

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Enter the super-VLAN configuration mode.	super-vlan *vlan-id*	-
Enable the ND proxy function	nd local-proxy enable	Mandatory By default, do not enable the ND proxy function.

Note

- The ND proxy function depends on the L3 forwarding function. If the device does not support the L3 IPv6 forwarding function, the ND proxy function does not take effect.

4.5.2.5 VLAN Monitoring and Maintaining

Table 268 Super-VLAN Monitoring and Maintaining

Command	Description
show super-vlan [*vlan-id*]	Display the information about the specified super-VLAN.
show super-vlan config { *vlan-id* | all }	Display Super-VLAN configuration information
show super-vlan [*vlan-id*] portlist	Display the managed port information in Super-VLAN
show super-vlan *vlan-id* sub-vlan *vlan-id* portlist	Display the managed port information in Sub-VLAN

4.5.3 Super-VLAN Typical Configuration Example

4.5.3.1 Configure a Super VLAN

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

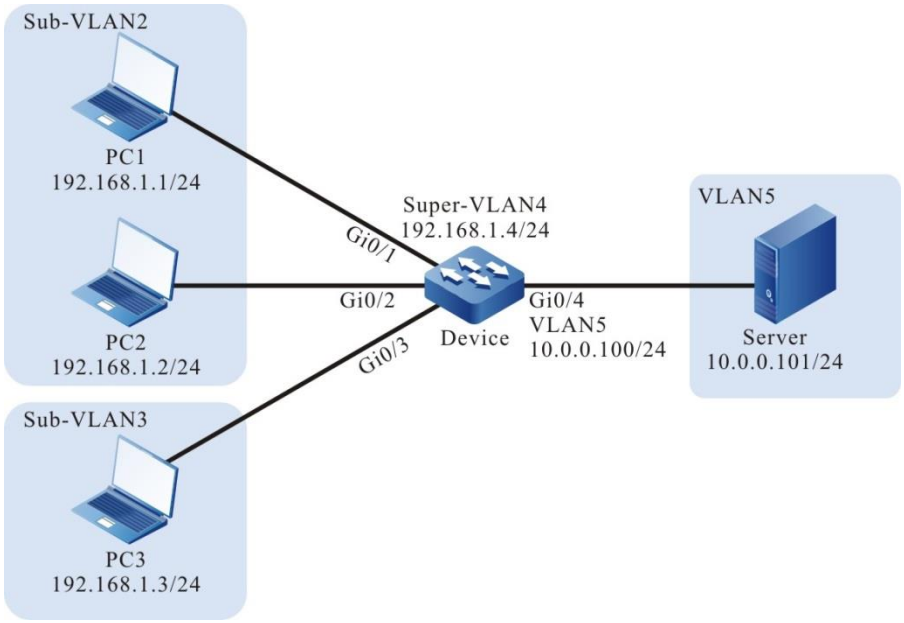


Figure 59 Networking for Configuring a Super-VLAN

Configuration Steps

Step 1: On Device, configure VLANs, and configure the port link types of the ports.

#On Device, create VLAN2, VLAN3, VLAN5.

```
Device#configure terminal
Device(config)#vlan 2-3,5
```

#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
```

Caution

- To enable the hosts in different sub-VLANs to communicate with each other at layer 3, the ARP proxy function must be enabled.
- Super-VLAN and Sub-VLAN should be in one spanning tree instance.

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.

4.6 PVLAN

4.6.1 Overview

To realize isolation between users but make the users still capable of accessing public resources, usually one VLAN needs to be created for one user. However, the total number of VLANs is only 4094, if the number of users is larger than the number of VLANs, the number of VLANs becomes a bottleneck. In addition, it is not easy to configure, manage, and maintain a large number of VLANs. To address the requirement, Private VLAN (PVLAN) emerges. It provides a flexible VLAN configuration mode in which VLAN and IP address resources can be reasonably allocated and used, simplifying network configuration.

In a PVLAN, a two-layer VLAN structure is used, that is, primary VLAN and secondary VLAN. Primary VLANs are usually connected to upstream devices, and secondary VLANs are usually connected to downstream devices. According to layer-2 forwarding rules, secondary VLANs are categorized into the following two types:

- Isolated VLAN: The member ports in an isolated VLAN are isolated from each other at layer 2, and the member ports from different isolated VLANs are also isolated from each other. To achieve isolation of users, you only need to add the ports to which the users are connected to isolate VLANs.
- Community VLAN: The forwarding rules of a community VLAN is the same as those of a common VLAN. The member ports in the same community VLAN can communicate with each other at layer 2, while the ports are isolated from member ports in other community VLANs or isolated VLANs.

After a primary VLAN sets up an association relation with secondary VLANs, the member ports in the secondary VLANs can communicate with the member ports in the primary VLAN at layer 2, and the member ports in the secondary VLANs can communicate with external devices at layer 3 through the VLAN interface of the primary VLAN.

PVLANs have two special port link types, Promiscuous and Host. Promiscuous ports can only be added into primary VLANs, and Host ports can only be added into secondary VLANs. The Host ports that are added into community VLANs are also called community ports, and the Host ports that are added into isolated VLANs are also called isolated ports.

4.6.2 PVLAN Function Configuration

Table 269 PVLAN Function List

Configuration Tasks	
Configure a primary VLAN.	Configure a primary VLAN.
Add ports into a primary VLAN.	Add ports into a primary VLAN.
Configure secondary VLANs.	Configure secondary VLANs.
Add ports into secondary VLANs.	Add ports into secondary VLANs.
Set up an association relation between a primary VLAN and secondary VLANs.	Set up an association relation between a primary VLAN and secondary VLANs.

4.6.2.1 Configure a Primary VLAN

The upstream devices recognize only the primary VLAN while they do not care about the associated secondary VLANs.

Configuration Condition

None

Configure a Primary VLAN

Table 270Configuring a Primary VLAN

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the VLAN configuration mode.	vlan *vlan-id*	-
Configure the VLAN to the primary VLAN type.	private-vlan primary	Mandatory. By default, all VLANs are common

Step	Command	Description
		VLANs.

4.6.2.2 Add Ports into a Primary VLAN

Only the ports whose link type is Promiscuous can be added into a primary VLAN. The ports that are added into a primary VLAN can communicate at layer two with the other member ports in the primary VLAN and the member ports of the associated secondary VLANs. Promiscuous ports are usually used as upstream ports.

Configuration Condition

Before adding ports into a primary VLAN, ensure that:

- The VLAN into which the ports are added is of the primary VLAN type.

Add Ports into a Primary VLAN

Table 271 Adding Ports into a Primary VLAN

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the layer-2 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.	**interface link-aggregation** *link-aggregation-id*	
Configure the port link type to Promiscuous.	**switchport mode private-vlan promiscuous**	Mandatory. By default, the port link type is the Access type.
Add Promiscuous ports into the	**private-vlan promiscuous** *vlan-*	Mandatory.

Step	Command	Description
primary VLAN.	*id*	By default, a Promiscuous port is not added into any VLAN.

Note

- If you configure a port link type to Promiscuous but do not add the port into a primary VLAN, the PVLAN function of the port does not take effect. In addition, the port of the Promiscuous type is dedicated for PVLAN, and the other functions that are configured on the Promiscuous port are invalid. Therefore, it is recommended that you follow the previous steps to complete the configuration.

4.6.2.3 Configure Secondary VLANs

The downstream devices recognize only secondary VLANs while they do not care about the associated primary VLAN.

Configuration Condition

None

Configure Secondary VLANs

Table 272 Configuring Secondary VLANs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the VLAN configuration mode.	vlan *vlan-id*	-
Configure VLANs to the secondary VLAN type.	private-vlan { community | isolated }	Mandatory. By default, all VLANs are

Step	Command	Description
		common VLANs.

4.6.2.4 Add Ports into Secondary VLANs

Only the ports whose link type is Host can be added to secondary VLANs. Secondary VLANs are categorized into two types: community VLANs and isolated VLANs. The ports that are added into a community VLAN can only communicate at layer 2 with the other member ports of the community VLAN and the member ports of the associated primary VLAN. The ports that are added into an isolated VLAN can only communicate at layer 2 with the member ports of the associated primary VLAN. Host ports are usually used as downstream ports.

Configuration Condition

Before adding ports into a secondary VLAN, ensure that:

- The VLAN into which the ports are added is of the secondary VLAN type.

Add Ports into Secondary VLANs

Table 273 Adding Ports into Secondary VLANs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enters the interface config mode.	interface *interface-name*	Either After you enter the 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
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		aggregation group.
Configure the port link type to the Host type.	switchport mode private-vlan host	Mandatory. By default, the port link type is the Access type.
Add Host ports into the secondary VLANs.	private-vlan host *vlan-id*	Mandatory. By default, a host port is not added into any VLAN.

Note

- The hosts in a secondary VLAN cannot communicate with the VLAN interface of the device at layer 3.
- If you configure a port link type to Host but do not add the port into a secondary VLAN, the PVLAN function of the port does not take effect. In addition, the port of the Host type is dedicated for PVLAN, and the other functions that are configured on the Host port are invalid. Therefore, it is recommended that you follow the previous steps to complete the configuration.

4.6.2.5 Set Up an Association Relation Between a Primary VLAN and Secondary VLANs

After an association relation is set up, the hosts in a primary VLAN can communicate at layer 2 with the host in the associated secondary VLANs. A primary VLAN can be associated with a maximum of one isolated VLAN and 192 community VLANs. One secondary VLAN can be associated only with one primary VLAN.

Configuration Condition

Before setting up an association relation between a primary VLAN and secondary

VLANs, ensure that:

- The VLAN in the current VLAN configuration mode is of the primary VLAN type.

Set Up an Association Relation Between a Primary VLAN and Secondary VLANs

Table 274 Setting Up an Association Relation Between a Primary VLAN and Secondary VLANs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the VLAN configuration mode.	vlan *vlan-id*	-
Set up an association relation between the primary VLAN and secondary VLANs.	private-vlan association add *vlan-list*	Mandatory. By default, a primary VLAN is not associated with any secondary VLAN.

Note

- If a primary VLAN is associated with a common VLAN, the association is invalid. To make the association take effect, modify the VLAN type to secondary VLAN.
- If a secondary VLAN is associated with a primary VLAN, the MAC address entries that are dynamically learned by the secondary VLAN are recorded in the FDB table as primary VLANs instead of secondary VLANs that are associated with the secondary VLAN.

4.6.2.6 PVLAN Monitoring and Maintaining

Table 275 PVLAN Monitoring and Maintaining

Command	Description
show private-vlan [*vlan-id*]	Displays the information about the PVLAN.

4.6.3 PVLAN Typical Configuration Example

4.6.3.1 Configure a PVLAN

Network Requirements

- PC1 and PC2 belong to secondary VLAN2, PC3 and PC4 belong to secondary VLAN3, and Server belongs to primary VLAN4.
- PVLAN is configured on Device. Then, interconnection is allowed within secondary VLAN 2, isolation is implemented within secondary VLAN3, secondary VLAN2 and secondary VLAN3 are isolated from each other, and secondary VLAN2 and secondary VLAN3 can interconnect with primary VLAN4.

Network Topology

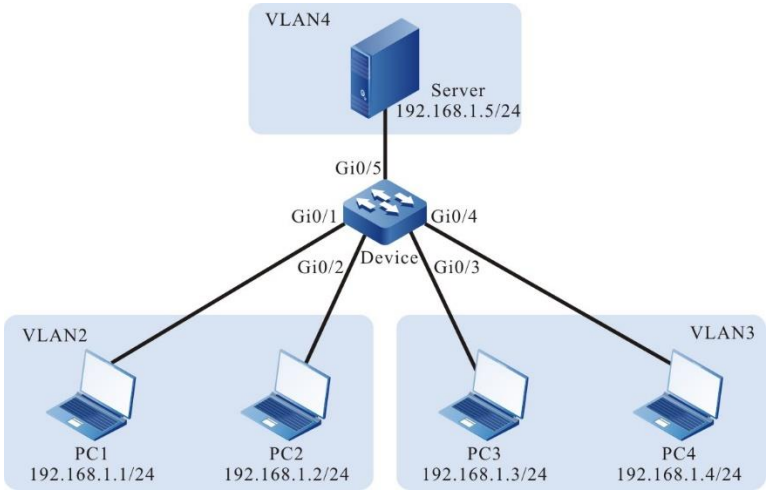


Figure 60 Networking for Configuring a PVLAN

Configuration Steps

Step 1: Configure VLANs on Device.

#On Device, create VLAN2-VLAN4.

```
Device#configure terminal
Device(config)#vlan 2-4
```

Step 2: On Device, configure the PVLAN function.

#On Device, configure VLAN4 to primary VLAN, configure VLAN2 to community VLAN, and configure VLAN3 to isolated VLAN.

```
Device(config)#vlan 4
Device(config-vlan4)#private-vlan primary
Device(config-vlan4)#vlan 2
Device(config-vlan2)#private-vlan community
Device(config-vlan2)#vlan 3
Device(config-vlan3)#private-vlan isolated
Device(config-vlan3)#exit
```

#On Device, associate primary VLAN4 with community VLAN2 and isolated VLAN3.

```
Device(config)#vlan 4
Device(config-vlan4)#private-vlan association add 2,3
Device(config-vlan4)#exit
```

#On Device, configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 to Host, and add the ports into secondary VLAN2.

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode private-vlan host
Device(config-if-range)#private-vlan host 2
Device(config-if-range)#exit
```

#On Device, configure the link type of ports gigabitethernet0/3 and gigabitethernet0/4 to Host, and add the ports into secondary VLAN3.

```
Device(config)#interface gigabitethernet 0/3-0/4
Device(config-if-range)#switchport mode private-vlan host
Device(config-if-range)#private-vlan host 3
Device(config-if-range)#exit
```

#On Device, configure the link type of port gigabitethernet0/5 to Promiscuous, and add the ports into primary VLAN4.

```
Device(config)#interface gigabitethernet 0/5
Device(config-if-gigabitethernet0/5)#switchport mode private-vlan promiscuous
```

```
Device(config-if-gigabitethernet0/5)#private-vlan promiscuous 4
Device(config-if-gigabitethernet0/5)#exit
```

Step 3: Check the result.

#Query the PVLAN information on Device.

```
Device#show private-vlan
---- -------- ---------- ---------------- ------------------------------ ------------
--------------------
NO.  Primary  Secondary  Type          Interface(Primary)           Interface(Secondary)
---- -------- ---------- ---------------- ------------------------------ ------------
--------------------
1    4        3          isolated      gi0/5                    gi0/3     gi0/4
2    4        2          community     gi0/5                      gi0/1     gi0/2
```

#PC1 and PC2 in community VLAN2 can ping each other successfully.

#PC3 and PC4 in isolated VLAN3 can ping each other successfully.

#PC1 and PC2 in community VLAN2 and PC3 and PC4 in isolated VLAN3 cannot ping each other.

#PC1 and PC2 in community VLAN2 can ping Server successfully.

#PC3 and PC4 in isolated VLAN3 can ping Server successfully.

4.7 Voice-VLAN

4.7.1 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.

4.7.2 Voice-VLAN Function Configuration

Table 276 Voice-VLAN Function List

Configuration Tasks	
Configure a voice-VLAN.	Configure a voice-VLAN.
Configure an OUI address.	Configure an OUI address.
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.
Enable the security mode of Voice-VLAN	Enable the security mode of Voice-VLAN
Enable the lldp-med authentication mode of Voice-VLAN	Enable the lldp-med authentication mode of Voice-VLAN

4.7.2.1 Configure a Voice-VLAN

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 Condition

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 277 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-

Step	Command	Description
		VLAN function is not globally enabled.

4.7.2.2 Configure an OUI Address

Configuration Condition

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 278 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 32 OUI addresses.

4.7.2.3 Enable the Voice-VLAN Function

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 Condition

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 279 Enabling the Voice-VLAN Function of a Port

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 voice-VLAN function of a port.	voice vlan enable	Mandatory. By default, the voice-VLAN function is disabled on the port.

Note

- The security mode of Voice-VLAN does not support aggregation group, that is, when the device enables the security mode of Voice-VLAN, the aggregation group cannot enable Voice-VLAN function; or when the device has the aggregation group enabled with the Voice-VLAN function, the security mode of Voice-VLAN cannot be enabled.
- The lldp-med authentication mode of Voice-VLAN does not support the aggregation group, that is, when the device enables the lldp-med authentication mode of Voice-VLAN, the aggregation group cannot enable the Voice-VLAN function; or when the device has the aggregation group enabled with the Voice-VLAN function, the lldp-med authentication mode of Voice-VLAN cannot be enabled.

4.7.2.4 Configure the Voice-VLAN Working Mode on the Port

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 or the Tag packet with the Voice-VLAN ID and the source MAC address of the packets matches an OUI address, the packets are regarded as voice packets.
- Manual mode: The packets received by the port are all regarded as voice packets.

Configuration Condition

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 280 Configuring a Voice-VLAN to Automatic 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 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 281 Configuring a Voice-VLAN to Manual 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
Enter the aggregation group configuration mode.	link-aggregation *link-aggregation-id*	

Step	Command	Description
		port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
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.

Note

- If the port is used to transmit the Tagged voice data, the port type can only be configured as Trunk or Hybrid, and PVID cannot be Voice-VLAN.
- If the port works in the Voice-VLAN manual mode, and is used to transmit the untagged voice data, PVID should be Voice-VLAN.
- The lldp-med authentication mode of Voice-VLAN does not support the manual mode of ports, that is, when the devices enable the lldp-med authentication mode of Voice-VLAN, the ports cannot be configured as the manual mode of Voice-VLAN; or when there is one port configured as the manual mode of Voice-VLAN, the lldp-med authentication mode of Voice-VLAN cannot be enabled.

4.7.2.5 Enable the Security Mode of Voice-VLAN

After enabling the security mode of Voice-VLAN, the device will check the source MAC address of each packet that enters Voice-VLAN for transmission, and discard the packet that cannot match the OUI address.

Configuration Condition

Before enabling the security mode of Voice-VLAN, complete the following task:

- Globally enable the Voice-VLAN function

Enable the Security Mode of Voice-VLAN

Table 6-282 Enable the security mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the security mode of Voice-VLAN	voice vlan security enable	Mandatory By default, do not enable the security mode of Voice-VLAN.

Note

- The security mode of Voice-VLAN does not support aggregation group, that is, when the device has the aggregation group enabled with the Voice-VLAN function, the security mode of Voice-VLAN cannot be enabled; or when the device enables the security mode of Voice-VLAN, the aggregation group cannot enable the Voice-VLAN function.

4.7.2.6 Enable lldp-med Authentication Mode of Voice-VLAN

After the lldp-med authentication mode of Voice-VLAN is enabled, the device takes the OUI configured by the user or default OUI as the authentication whitelist, performing the matching check for the source MAC address of the voice device notified by lldp-med, and the voice packets sent by the voice device that matches the whitelist can enter Voice-VLAN for transmission.

Configuration Condition

Before enabling the lldp-med authentication mode of Voice-VLAN, complete the

following task:

- Globally enable the Voice-VLAN function

Enable the lldp-med Authentication Mode of Voice-VLAN

Table 6-283 Enable the lldp-med authentication mode of Voice-VLAN

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the lldp-med authentication mode of Voice-VLAN	voice vlan lldp-med authentication	Mandatory By default, do not enable the lldp-med authentication mode of Voice-VLAN

Note

- The lldp-med authentication mode of Voice-VLAN does not support the aggregation group, that is, when the device has the aggregation group enabled with the Voice-VLAN function, the lldp-med authentication mode of Voice-VLAN cannot be enabled; or when the device enables the lldp-med authentication mode of Voice-VLAN, the aggregation group cannot enable the Voice-VLAN function.
- The lldp-med authentication mode of Voice-VLAN does not support the manual mode of ports, that is, when there is one port configured as the manual mode of Voice-VLAN, the lldp-med authentication mode of Voice-VLAN cannot be enabled; or when the device enables the lldp-med authentication mode of Voice-VLAN, the port cannot be configured as the manual mode of Voice-VLAN.
- After the lldp Med authentication mode of voice VLAN is enabled, the telephone that does not support lldp cannot work normally.

4.7.2.7 Voice-VLAN Monitoring and Maintaining

Table 284 Voice-VLAN Monitoring and Maintaining

Command	Description
show voice vlan { all | interface [*interface-name*] | link-aggregation [*link-aggregation-id*] | oui | lldp-med authenticated-mac }	Displays the information about the voice-VLAN.

4.7.3 Voice-VLAN Typical Configuration Example

4.7.3.1 Configure a Voice-VLAN to Manual Mode

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

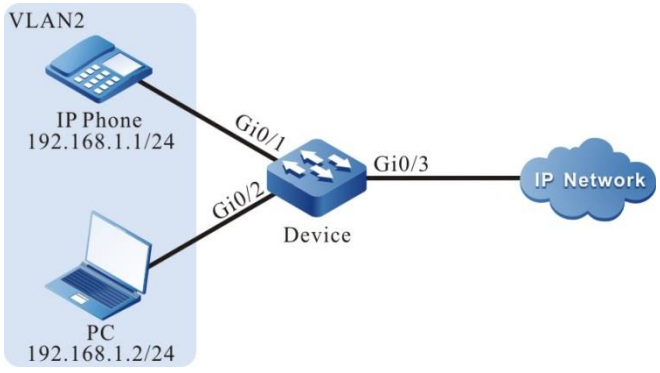


Figure 61 Networking for Configuring a Voice-VLAN to Manual Mode

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 security:  disable
 Voice Vlan lldp-med authentication:  disable
 Voice Vlan VID: 2, Cos: 7
 Default OUI number: 5
 User config OUI number: 0

 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
```

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.

4.7.3.2 Configure a Voice-VLAN to Automatic Mode

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

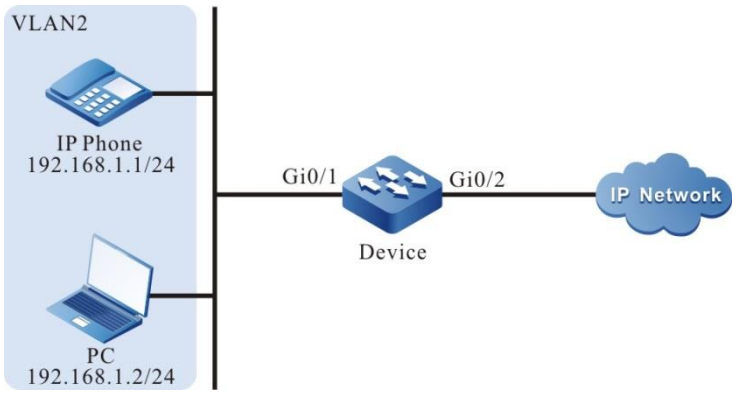


Figure 62 Networking for Configuring a Voice-VLAN to Automatic Mode

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 Trunk and allow services of VLAN2 to pass.

```
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
```

#On Device, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN2 to pass.

```
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 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 security:  disable
 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 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.

4.7.3.3 Configure the Security Mode of Voice-VLAN

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.
- On Device, configure the security mode of Voice-VLAN, realizing that IP Phone can access IP Network normally, and PC cannot access IP Network.

Network Topology

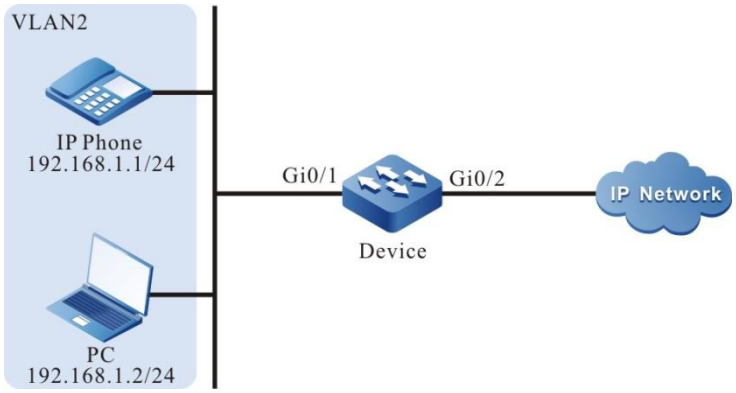


Figure 63 Networking for Configuring the security mode of Voice-VLAN

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 Trunk and allow services of VLAN2 to pass.

```
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
```

#On Device, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN2 to pass.

```
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 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 Device, globally enable the security mode of Voice-VLAN.

```
Device(config)# voice vlan security enable
```

#On port gigabitethernet0/1 of Device, configure the voice-VLAN auto 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 of 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, view the 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 802.1 priority of the packets that IP Phone sends to IP Network is modified to 7.

PC cannot normally access IP Network.

4.7.3.4 Configure lldp-med Authentication Mode of Voice-VLAN

Network Requirements

- IP Phone (the IP phone can send the LLDP packet with the voice field) 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.
- Ton Device, configure the lldp-med authentication mode of Voice-VLAN so that IP Phone can normally access IP network and PC cannot access IP Network.

Network Topology

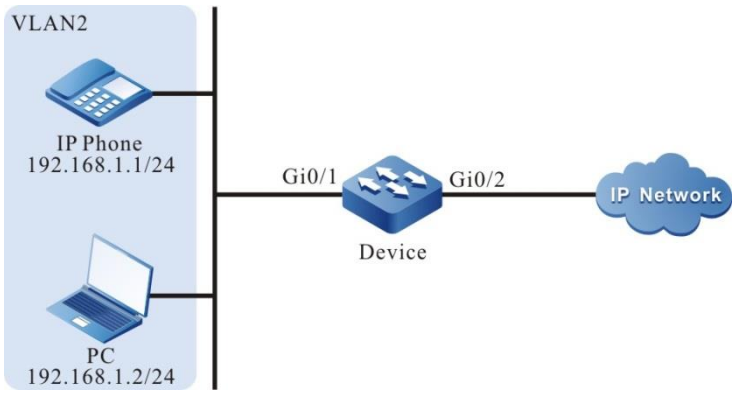


Figure 64 Networking for Configuring the lldp-med authentication mode of Voice-VLAN

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 Trunk and allow services of VLAN2 to pass.

```
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
```

#On Device, configure the link type of port gigabitethernet0/2 to Trunk and allow services of VLAN2 to pass.

```
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 the Voice-VLAN function.

#On Device, configure VLAN2 as Voice-VLAN, and the modify the Cos value to 7.

```
Device(config)#voice vlan 2 cos 7
```

#On Device, globally enable the lldp-med authentication mode of Voice-VLAN.

```
Device(config)#voice vlan lldp-med authentication
```

#On port gigabitethernet0/1 of Device, configure the Voice-VLAN auto 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 of the MAC address of IP Phone

0001.0001.0001.

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#On Device, view the 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 802.1P priority of the packet sent by IP Phone to IP Network is modified to 7.

#PC cannot access IP Network.

4.8 MAC Address Table Management

4.8.1 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 data packet, 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.

4.8.2 MAC Address Management Function Configuration

Table 285 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.

Configuration Tasks	
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.
	Configure the static forwarding MAC address of multiple outgoing interfaces

4.8.2.1 Configure Management Properties of MAC Addresses

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 Condition

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.
- 60-1000000: 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 286 Configuring the MAC Address Aging Time

Step	Command	Description
Enter the global configuration mode.	configure 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 MAC Migration Inhibition Function

By default, the MAC address migration inhibition function is disabled in the port. At this time, the port normally learns the MAC address table entry and forwards the corresponding packet; If the MAC address migration inhibition function is enabled under the port, the MAC learned by the port will be detected for address migration. If it is detected that the MAC address of the port has migrated beyond the normal

conditions, you can make a policy for the migrated MAC. The policy control includes speed limit learning for the migrated MAC and errdisable down for the port.

Table 287 Configure the MAC address migration inhibition 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.	interface link-aggregation *link-aggregation-id*	
Enable the MAC address migration inhibition function of the port or aggregation group	mac-address flapping policy errdisable	Mandatory By default, the port disables the MAC address migration function.
Global configuration mode	mac-address flapping detection threshold *threshold-count*	Optional Configure the detection threshold. The maximum times of allowed address migrations in the detection cycle. If exceeding the times, it is considered that the MAC has a migration exception and a policy needs to be made.
Global configuration mode	mac-address flapping detection interval *interval-time*	Optional Configure the detection threshold. The maximum times of allowed address migrations in the detection cycle. If exceeding the times, it is considered that the MAC has a migration exception and a policy

Step	Command	Description
		needs to be made.
Global configuration mode	mac-address flapping policy rate-limit level *level*	Optional After detecting the address migration exception, perform the speed limit processing for the MAC, used for optimizing CPU.

Note

- By default, port ErrDisable Down of the address migration inhibition is disabled. To enable it, you need to enable ErrDisable of the address migration.

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 288 Configuring the MAC Address Learning Capability

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
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		aggregation group configuration mode, the subsequent configuration takes effect only on 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.

Configure the MAC Address Learning Function

Enable/disable the MAC address learning function is valid for learning the dynamic MAC address and forwarding the packet. By default, the MAC address learning function is enabled on the port, and the port can learn the MAC address entry, and forward the packet. If the MAC address learning function is disabled on the port, the port does not learn the dynamic MAC address any more, but still can forward the packet.

Table 289 Configuring MAC address learning function

Step	Command	Description
Enter the 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 takes effect only on the current port. After entering the aggregation group configuration mode, the subsequent configuration takes
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		effect only on the aggregation group.
Enable the learning function of the port or aggregation group MAC address	mac-address learning action forward	Mandatory By default, enable the MAC address learning function on the port.

4.8.2.2 Configure Limitations on MAC Address Learning

Limitations on MAC address learning is categorized into two types: limitations on port-based dynamic MAC address learning, and limitations on VLAN-based dynamic 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 Condition

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 290 Configuring Limitations on Port-Based Dynamic MAC Address Learning

Step	Command	Description
Enter the 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 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.	interface 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 range of the maximum number of the dynamic learned MAC addresses is from 1 to the maximum address entries the hardware chip can learn.

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 291 Configuring Limitations on VLAN-Based Dynamic MAC Address Learning

Step	Command	Description
Enter the global configuration mode.	configure 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 range of the maximum number of the dynamic learned MAC addresses is from 1 to the maximum address entries the hardware chip can learn.

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.

4.8.2.3 Configure Static MAC Addresses

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 addresses.

One MAC address can only be configured as a static forwarding MAC address or a static filtering MAC address in a VLAN.

Configuration Condition

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 292 Configuring Static Filtering MAC Addresses

Step	Command	Description
Enter the global configuration mode.	configure 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 293 Configuring Static Forwarding MAC Addresses That Are Bound to a Port

Step	Command	Description
Enter the global configuration mode.	configure 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 294 Configuring Static Forwarding MAC Addresses That Are Bound to an Aggregation Group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure static forwarding MAC addresses that are bound to an aggregation group.	mac-address static *mac-address-value* vlan *vlan-id* interface 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.

4.8.2.4 MAC Address Management Monitoring and Maintaining

Table 295 MAC Address Management Monitoring and Maintaining

Command	Description
clear mac-address dynamic { mac-address-value | all | interface interface-list | interface link-aggregation link-aggregation-id | vlan vlan-id [mac-address-value | interface interface-list | interface 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 the MAC address entry information in the port
show mac-address interface 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 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.
show mac-address max-mac-count { interface interface-name | interface 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 | interface link-aggregation link-	Displays MAC address entry statistics in the system.

Command	Description
aggregation-id | vlan vlan-id]	

4.8.3 Software Learning Function Configuration

4.8.3.1 Software Learning Function Configuration

After the software learning function is enabled, learn the MAC address entry through the software.

Configuration Condition

No

Enable Software Learning Function

Table 296 Enable the software learning function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the software learning function	mac-address software-learning enable	By default, it is disabled.

Disable Software Learning Function

Table 297 Disable the software learning function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Disable the software learning function	no mac-address software-learning enable	After disabling the software learning, learn the MAC address entry is learned via the chip.

Note

- In standalone mode, it is hardware learning by default. If you configure this command, you can switch to software learning, but you need to restart the device to take effect.
- In stack mode, it is software learning by default, and it is not recommended to switch to hardware learning.
- The MLAG function only supports software learning, not supporting hardware learning.

4.8.3.2 Software Learning Function Monitoring and Maintaining

Table 298 Software Learning Monitoring and Maintaining

Command	Description
show mac-address software-learning	View whether the software learning is enabled or disabled

4.8.4 MAC Address Moving Log Function Configuration

4.8.4.1 Configure MAC Address Moving Log Function

The MAC address moving log function can be enabled and disabled manually. After enabling the MAC address moving log function, record one address moving log when the address of the MAC address entry moves.

Configuration Condition

None

Enable MAC Address Moving Log Function

Table 299 Enable the MAC address moving log function

Step	Command	Description
Enter the global configuration mode.	config terminal	-
Enable the address moving log function	mac-address move log	By default, it is enabled.

Disable MAC Address Moving Log Function

Table 300 Disable the MAC address moving log function

Step	Command	Description
Enter the global configuration mode.	config terminal	-
Disable the MAC address moving log function	no mac-address move log	After disabling the address moving log function, do not record the log information when the address of the MAC address entry moves.

4.8.4.2 Monitoring and Maintaining of MAC Address Moving Log Function

Table 301 MAC address moving monitoring and maintaining

Command	Description
clear mac-address move log{*mac-address*}	Clears the MAC address moving logs
show mac-address move config	Displays the configuration information of the MAC address moving log function
show mac-address move log {*mac-address-value* | count *count* | hardlearn | start-time [*time*] end-time [*time*] }	Displays the MAC address moving log

4.9 Spanning Tree

4.9.1 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 spanning tree 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. SOFINET implements the VIST and Rapid-VIST spanning tree protocols compatible with Cisco spanning tree. Rapid-VIST improves convergence performance and inherits the function of VIST ring elimination.

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 spanning tree 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 spanning tree 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 spanning tree 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 spanning tree 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 cause re-calculation of the spanning tree 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 spanning tree, which has the following shortages:

- Only one spanning tree 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 spanning tree, 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 spanning tree. 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 spanning tree 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 spanning tree of instance 0 in each region.
- Common Spanning Tree (CST): If each MST region is regarded as a device, then the spanning trees 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 spanning tree that connects all devices in the network.
- Multiple Spanning Tree Instance (MSTI): Spanning trees in MST regions. Each instance has an independent MSTI.
- Common root: CIST root.
- Region root: Root of each IST and MSTI in MST regions. In MST domains, each instance has an independent spanning tree, 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 MSTI 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 spanning tree instances, each MST region calculates an independent spanning tree MSTI for each instance.

Cisco private spanning tree protocol defines PVST and RPVST protocols, both of which introduce the concept of instance. A VLAN corresponds to an instance. In different instances, ports can have different port roles and port states, which realizes the packet forwarding of different VLANs according to their paths.

New definition of MSTP in MLAG environment and precautions:

- MLAG-MSTI: The corresponding MSTI instance of MLAG-VLAN
- root priority: The specified root bridge priority of MLAG
- bridge priority: The specified bridge priority of MLAG
- stp-pseudo: The pseudo information mode

The configuration restrictions of the pseudo information mode:

- The root priority (default value is 0) of CIST and all MLAG-MSTI in the pseudo information must be better than the bridge priority of all bridges (including MLAG nodes themselves) in the whole network (the default value is 32768);
- In addition to ensuring that the pairing node is the root bridge (root priority is the best in the whole network), it is also necessary to start the root guard function on the access ports (all non-peer link ports) of MLAG nodes (root guard has not been supported in vist mode) to prevent spanning tree calculation errors caused by receiving BPDU with higher priority.
- The Bridge-Assurance function needs to be configured on the peer link.
- For the CIST instance and MLAG-MSTI instance, the root priority of the two nodes must be configured to be the same, so that the two nodes present the same root bridge for both DHD and SD; in order to make the two nodes present two completely independent network bridges for SD to participate in

spanning tree calculation, the root priority of the two nodes must be configured differently

4.9.2 Spanning Tree Function Configuration

Table 302 Spanning Tree Function List

Configuration Tasks	
Configure basic functions of the spanning tree.	Enable the spanning tree function.
	Configure MST domain.
	Configure the spanning tree log output function
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 domain.
Configure spanning tree port properties.	Configure the priority of a port.
	Configure the default path cost standard for a port.
	Configure the path cost of a port.
	Configure the BPDU packet length check
	Configure the maximum length of the BPDU packet
	Configure the maximum transmitting rate of the BPDU packet
	Configure the source mac check of the BPDU packet
	Configure the timeout factor of the BPDU packet

Configuration Tasks	
	Configure an edge port.
	Configure the auto detection of the edge port
	Force the auto detection of the edge port
	Configure the port link type.
Configure the working mode of a spanning tree.	Configure the working mode of a spanning tree.
Configure the spanning tree 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 Guard function.
	Configure the TC protection function.

4.9.2.1 Configure Basic Functions of a Spanning Tree

Configuration Condition

None

Enable the Spanning Tree Function

After the spanning tree function is enabled, devices start to run the spanning tree protocol. The devices exchange BPDU packets to form a stable tree network topology, and network loops are eliminated.

Table 303 Enabling the Spanning Tree Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enabling the spanning tree function globally.	spanning-tree enable	Mandatory. By default, the spanning tree

Step	Command	Description
		function is disabled globally.
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.	interface link-aggregation *link-aggregation-id*	
Enabling the spanning tree function on a port.	spanning-tree enable	Optional. By default, the spanning tree 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 MSTIs in MST regions and transmitted through CSTs between MST regions.

Table 304 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.
Configure the MSTP revision level.	revision-level *revision-level*	Mandatory. By default, the MSTP

Step	Command	Description
		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 spanning tree. To cancel MST region parameter configuration, use the **abort configuration pending** command.

Configure Spanning Tree Log Output Function

After configuring the spanning tree log output function, the spanning tree will directly output the prompt log on the device if the port status changes or TC/TCN packet is received, so that users can quickly find the changes of topology environment.

Table 305 Enable the spanning tree function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the spanning tree log output function	spanning-tree log portstate	Mandatory By default, do not enable the spanning tree log output function.

4.9.2.2 Configure Bridge Properties

Configuration Condition

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 spanning tree instances.

Table 306 Configuring the Priority of a Bridge

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
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 spanning tree instances is 32768.
In the vist/rapid-vist mode, configure the priority of the bridge	spanning-tree vlan *vlan-id* priority *priority-value*	Mandatory By default, the bridge priority of the device in all spanning tree instances is 32768.

Note

- The step of bridge priorities is 4096, that is, the valid values include: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 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 spanning tree topology according to the BPDU packet, and it forwards the BPDU packet to other devices. Usually, if the designated bridge does not receive BPDU packets within three times of timeout (3*Hello Time), it regards the link as faulty. In this way, the spanning tree re-calculates the network topology to obtain a new active path, ensuring the network connectivity.

Table 307 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.
In vist/rapid-vist, configure Hello Time	spanning-tree vlan *vlan-id* hello-time *seconds*	Mandatory By default, the Hello Time is 2s.

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 308 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.
In the vist/rapid-vist mode, configure Forward Delay	spanning-tree vlan *vlan-id* 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 plus 1 is equal to the value of Max Age, the device discards the configuration message, and the configuration message is no longer used in spanning tree calculation.

Table 309 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.
In vist/rapid-vist mode, configure Max Age	spanning-tree vlan vlan-id 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 spanning tree calculation in the region.

Table 310 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.

4.9.2.3 Configure Spanning Tree Port Properties

Configuration Condition

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 spanning tree instances.

Table 311 Configuring the Priority of a Port

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.	interface link-aggregation *link-aggregation-id*	
Configure 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 spanning tree instances is 128.
In the vist/rapid-vist mode, configure the priority of a port.	spanning-tree vlan *vlan-id* port-priority *priority-value*	Mandatory. By default, the priority of the port in all spanning tree 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 312 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.	spanning-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 spanning tree instances.

Table 313 Configuring the Path Cost of a Port

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.	interface link-aggregation *link-aggregation-id*	
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.
In the vist/rapid-vist mode,	spanning-tree vlan *vlan-id*	Mandatory

Step	Command	Description
configure the path cost of the port	cost *cost-value*	By default, the path cost is automatically calculated according to the port rate.

Configure Length Check of BPDU Packet

Configuring the length check of the BPDU packet can let the port check the length of the received BPDU packet, so as to prevent the attack of the BPDU packet with the invalid length.

Table 314 Configure the length check of the BPDU packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the length check of the BPDU packet	spanning-tree bpdu length-check	Mandatory By default, do not enable the length check of the BPDU packet.

Configure Maximum Length of BPDU Packet

Configure the maximum length of the valid BPDU packet when checking the length of the BPDU packet.

Table 315 Configure the maximum length of the BPDU packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the maximum length of the BPDU packet	spanning-tree bpdu max-length *max-length*	Mandatory By default, the maximum length is 1500 bytes.

Configure 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 spanning tree calculation for other devices.

Table 316 Configuring the Maximum Transmitting Rate of BPDU Packets

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
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 Source MAC Check of BPDU Packet

Configuring the source mac check of the BPDU packet can let the port check the source MAC of the received BPDU packet, so as to prevent the BPDU packet attack of the invalid device.

Table 317 Configure the source mac check of the BPDU packet

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	interface link-aggregation *link-aggregation-id*	
Configure the source mac check of the BPDU packet	spanning-tree bpdu src-mac-match *src-mac*	Mandatory By default, the port does not enable the source MAC check

Step	Command	Description
		of the BPDU packet.

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 within three times of the timeout (3*HELLO TIME), it is considered that the network topology changes, which will start a spanning tree 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 a spanning tree re-election. In this case, you can configure the timeout factor to avoid such calculation.

Table 318 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 *times-number*	By default, if the device doesn't receive the BPDU packet from upper devices within three times of the timeout (3*HELLO TIME), it is considered that the network topology changes, which will start a spanning tree re-election. In stacking environment, it is recommended to configure the timeout factor as 6.
In the vist/rapid-vist mode, configure time factor of BPDU packets	spanning-tree vlan vlan-id timer-facor *times-number*	By default, if the device doesn't receive the BPDU packet from upper devices within three times of the timeout (3*HELLO TIME), it is considered that the

Step	Command	Description
		network topology changes, which will start a spanning tree 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 spanning tree 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 319 Configuring Global Edge Ports

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure an edge port.	spanning-tree portfast edgeport	Mandatory. By default, a port is a not an edge port.
Configure global edge port	spanning-tree edgeport enable	Mandatory By default, the global edge port is disabled.

Table 320 Configure the edge port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface	interface *interface-name*	Either

Step	Command	Description
configuration mode		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	interface link-aggregation *link-aggregation-id*	
Configure the edge port	spanning-tree portfast edgeport	Mandatory By default, the global edge port is not configured, and the port is the non-edge port; the global edge port is configured, and the port is the edge port.

Note

- Before specifying the port as the edge port, confirm whether the port is directly connected with the user terminal. Otherwise, it may cause the temporary loop after configuring as the edge port.
- Whether the spanning tree edge port is effective or not depends on the port configuration. When the port is not configured, if the global edge port is enabled, the edge port of the port is enabled by default; otherwise, the edge port of the port is disabled by default.

Configure Auto Detection of Edge Port

Configuring the auto detection of the edge port can let the port connected to the terminal automatically identified as edge port, so as to prevent the online/offline of the

terminal device from making the spanning tree re-calculation cause the network shock.

If receiving the BPDU packet after being identified as the edge port, it changes to the non-edge port again.

Table 321 Configure the auto detection of the edge port

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	interface link-aggregation *link-aggregation-id*	
Configure the auto detection of the edge port	spanning-tree portfast autoedge	Mandatory By default, the auto detection of the edge port is enabled in the single-machine mode, and is disabled in the stacking mode.

Force Auto Detection of Edge Port

Because of the configuration or environment, the current port may be identified as the edge port or non-edge port wrongly. Here, the user can execute the command to trigger the port to perform the edge port detection so that the port can identify whether itself is the edge port correctly.

Table 322 Configure the auto detection of the edge port

Step	Command	Description
Enter the 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 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	interface link-aggregation *link-aggregation-id*	
Force the auto detection of the edge port	spanning-tree portfast autoedge force	Mandatory

Note

- The command can take effect only when the port enables the auto edge port detection.

Configure 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 323 Configuring the Port Link Type

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
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		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 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 duplex mode, the port is set to the shared link type.

Note

- The port link type should be configured according to the actual physical link. If the actual physical link of the port is not point-to-point link, and is configured as the point-to-point link wrongly, it may cause the temporary loop.
- When the local port link type is the share link type, the local port does not support the auto identifying function of the edge port. If the peer port performs the auto identifying of the edge port, it may make the peer port be identified as the edge port wrongly.

Configure Port Bridge Assurance Function

After the bridge assurance function is enabled on the current port, the port will send BPDU regardless of its spanning tree role (even AlternatePort or BackupPort). If

the port does not receive BPDU from the peer device for a period of time, the port state will switch to the Blocking state and will not participate in spanning tree calculation. If the BPDU of the peer device is received in the future, the current port will resume normal spanning tree calculation.

Table 324 Configure the port Bridge Assurance 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.	interface link-aggregation *link-aggregation-id*	
Configure the port Bridge Assurance function	spanning-tree bridge-assurance enable	Mandatory By default, the Bridge Assurance function of the port is not enabled.

Note

- The configuration restrictions of Bridge-Assurance:
- It is mutually exclusive with BPDU-Guard, BPDU-Filter, Port-Fast (adminEdge, autoEdge) of the port. If one of these functions is configured on the port, Bridge-Assurance cannot be configured (there will be a print prompt).
- In STP mode, RP and AP cannot send BPDU at will, so the Bridge-

Assurance configuration in STP mode is not effective, but can be configured.

4.9.2.4 Configure Working Mode of a Spanning Tree

The working mode of a spanning tree 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 Condition

None

Configure the Working Mode of a Spanning Tree

Table 325 Configuring the Working Mode of a Spanning Tree

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the working mode of a spanning tree.	spanning-tree mode { stp | rstp | mstp | vist | rapid-vist}	Mandatory. By default, the working mode of a spanning tree is MSTP.

4.9.2.5 Configure the Spanning Tree Protection Function

Configuration Condition

None

Configure 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 spanning tree. 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 326 Configure the global BPDU Guard function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable global BPDU Guard	spanning-tree bpdu-guard enable	Mandatory By default, the global BPDU Guard is not enabled.

Table 327 Configuring the BPDU Guard 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.	interface link-aggregation *link-aggregation-id*	
Configure the BPDU Guard function.	spanning-tree bpdu guard enable	Mandatory. By default, the global BPDU guard is not configured, and the

Step	Command	Description
		BPDU Guard function of the port is disabled; the global BPDU guard has been configured, and the BPDU Guard function of the port is enabled.

Note

- Whether the BPDU guard function of spanning tree port is effective or not depens on the port configuration. When the port is not configured, if the global BPDU guard is enabled, the port BPDU guard function is enabled by default; otherwise, the port BPDU guard function is disabled by default.

Configure BPDU Filter Function

After the BPDU Filter function is enabled on an edge port, the port does not send or receive BPDU packets.

Table 328 Configuring the global BPDU Filter Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the global BPDU Filter function.	spanning-tree bpdu-filter enable	Mandatory. By default, the global BPDU Filter function is disabled.

Table 329 Configuring the BPDU Filter 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

Step	Command	Description
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	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.
Configure the BPDU Filter function.	spanning-tree bpdu filter enable	Mandatory. By default, the global BPDU filter is not configured, and the BPDU filter function of the port is disabled; The global BPDU filter has been configured, and the BPDU filter function of the port is enabled.

Note

- Whether the BPDU filter function of the spanning tree port is effective or not depends on the port configuration. When the port is not configured, if the global BPDU filter is enabled, the port BPDU filter function is enabled by default; otherwise, the port BPDU filter function is disabled by default.

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 a spanning tree 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 spanning tree calculation only after the recovery time times out.

Table 330 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 recovery-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 spanning tree 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 spanning tree calculation. If an instance on the port receives BPDU packets again, the port participates in spanning tree calculation again.

Table 331 Configuring the Loop Guard 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.	interface 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 a spanning tree 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.

Table 332 Configuring the Root Guard 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.	interface 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 TC Guard Function

When the device detects the network topology change, generate the TC packet and inform the other devices in the environment that the network topology changes. After the device receives the TC packet, refresh the address. When the topology is not stable or constructing the TC packets artificially to attack, generate TC frequently in the network and as a result, the device refreshes the address repeatedly, affecting the spanning tree calculation and resulting in the high CPU occupation.

TC GUARD can prevent the case. After configuring TC GUARD on the current port and the device receives the TC packet, do not process the TC flag or spread TC any more, so as to prevent the TC packets from attacking the network efficiently.

Table 333 Configure TC Guard 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	interface link-aggregation *link-aggregation-id*	
Configure the TC Guard function	spanning-tree tc-guard enable	Mandatory By default, do not enable the TC

Step	Command	Description
		Guard function of the port.

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 spanning tree 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 334 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 disabled.
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 1.

4.9.2.6 Configure Pseudo Information Configuration Function of Spanning Tree

Configuration Condition

The spanning tree pseudo information is applied in the MALG environment. On the MALG virtual node, the conventional priority configuration method of the spanning tree will not be effective. Modify the priority of the instance corresponding to the MALG node by configuring the pseudo information of the spanning tree. At this time, the instance priority information of the BPDU sent by the MLAG GROUP is the pseudo information of the spanning tree we configured, ensuring that two MLAG node devices are externally presented as a spanning tree calculation of one device. Note that during configuration, ensure that the spanning tree pseudo information configuration on the MLAG active and standby devices is consistent, and the configured parameters in the pseudo information configuration mode only take effect in the MLAG environment.

Configure the Specified Root Bridge Priority of the Instance

Configure the root bridge priority of the specified spanning tree instance in the pseudo information.

Table 335 Configure the specified root bridge priority of the instance

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure entering the pseudo information	spanning-tree pseudo-information	Mandatory
Configure the root bridge priority of the specified spanning tree instance	mst instance *instance-id* root-priority *priority-value*	Mandatory By default, configure the root bridge priority of each spanning tree instance in the configuration pseudo information as 0 (the highest

		priority). *instance-id*: spanning tree instance ID, with a value range of 0 – 63. *priority-value*: configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority

Note

- The configuration step of root bridge priority value is 4096, which can be configured as: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
- On the MLAG paired device, the root bridge priorities of all instances configured in the pseudo information of the two devices must be consistent.

Configure Specified Bridge Priority of the Instance

Configure the specified bridge priority of the spanning tree instance in the configuration pseudo information.

Table 336 Configure the specified bridge priority of the instance

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure entering the pseudo information	spanning-tree pseudo-information	Mandatory
Configure the specified bridge priority of the specified spanning tree instance in the pseudo	mst instance *instance-id* designated-priority *priority-value*	Mandatory By default, configure the specified bridge priority for each spanning tree instance in

Step	Command	Description
information		the pseudo information as 32768. *instance-id*: The spanning tree instance ID, the value range is 0-63 *priority-value*: Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority

Note

- The configuration step of the specified bridge priority value is 4096, which can be configured as: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

Configure Root Bridge Priority of Specified VLAN List

Configure the root bridge priority of the device in the specified VLAN list.

Table 337 Configure the root bridge priority of the specified VLAN list

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure entering the pseudo information	spanning-tree pseudo-information	Mandatory
Configure the root bridge priority of the device in the specified VLAN list	vist vlan *vlan-list* root-priority *priority-value*	Mandatory By default, configure the root bridge priority of each VLAN

Step	Command	Description
		in the pseudo information as 0 (the highest priority). *priority-value*: Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority

Note

- The configuration step of root bridge priority value is 4096, which can be configured as: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.
- On the MLAG paired device, the root bridge priorities of all VLANs configured in the pseudo information of the two devices must be consistent.

Configure Bridge Priority of Specified VLAN List

Configure the bridge priority of the device in the specified VLAN list.

Table 338 Configure the bridge priority of the specified VLAN list

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure entering the pseudo information	spanning-tree pseudo-information	Mandatory
Configure the bridge priority of the device in the specified VLAN list	vist vlan *vlan-list* designated-priority *priority-value*	Mandatory By default, configure the specified bridge priority of each spanning tree instance in

Step	Command	Description
		the pseudo information as 32768. *priority-value*: Configure the root bridge priority of the device in the specified spanning tree instance. The smaller the value, the higher the priority

Note

- The configuration step of the specified bridge priority value is 4096, which can be configured as: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.

4.9.2.7 Spanning Tree Monitoring and Maintaining

Table 339 Spanning Tree Monitoring and Maintaining

Command	Description
clear spanning-tree detected-protocols	Perform the mcheck operation globally or on the specified port
clear spanning-tree bpdu statistics [interface interface-name | interface link-aggregation *link-aggregation-id*]	Clear all BPDU statistics information or on the specified port
show spanning-tree [detail]	Display the basic information of the spanning tree
show spanning-tree guard [current [interface *interface-name* | interface link-aggregation *link-aggregation-id*]]	Display the configuration and status information of the spanning tree protection function on the port
show spanning-tree { interface *interface-name* | interface link-aggregation *link-aggregation-id* } [detail]	Display the spanning tree status information of the specified port or aggregation group

Command	Description
show spanning-tree mst [configuration [current | pending] | detail | instance *instance-id* [detail] | { interface *interface-name* | interface link-aggregation *link-aggregation-id* } [instance *instance-id*]]	Display the configuration and status information about the spanning tree.
show configuration { current | pending }	Display the configuration of MST regions.
show spanning-tree vlan *vlan-id* [detail]	In the vist/rapid-vist mode, display the spanning tree status information of the specified VLAN

4.9.3 Spanning Tree Typical Configuration Example

4.9.3.1 MSTP Typical Application

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

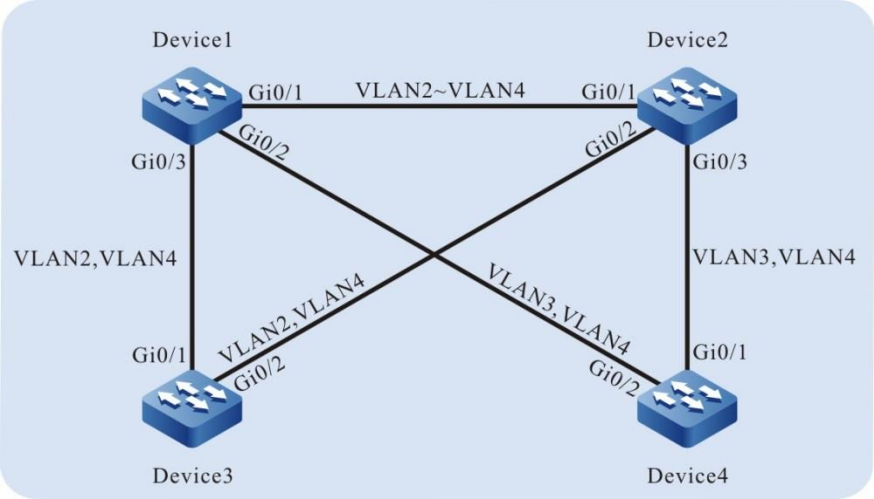


Figure 65 Networking for MSTP Typical Application

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 MSTI 1 to 0. On Device2, configure the priority of MSTI 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 spanning tree globally.
Device1(config)#spanning-tree enable
```

Note

- The configuration for enabling the spanning tree 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 spanning tree 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
 Bpdu length-check:  false, bpdu illegal length packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 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 0101.7a54.5c96 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 spanning tree 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 Instance 00        vlans mapped:  1,4-4094
 Bridge              address 0101.7a54.5c96 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
 Bpdu length-check: false, bpdu illegal length packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 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 0101.7a54.5c96 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 0101.7a54.5c96 priority 2/0
 Designated root      address 0101.7a54.5c96 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 spanning tree instances.

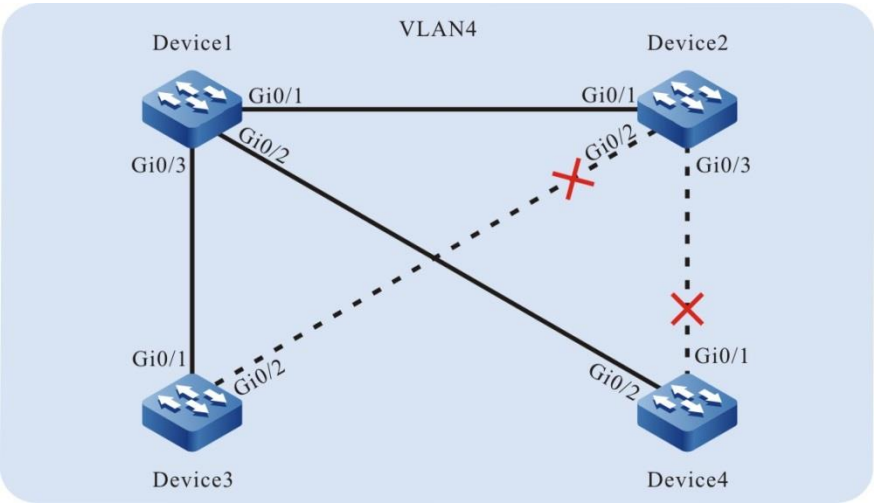
```
Device3#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00         vlans mapped: 1,4-4094
 Bridge              address 0000.0305.070a priority 32768
 Region root         address 0000.0000.008b priority 32768
Designated root      address 0000.0000.008b priority 32768
                  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
 Bpdu length-check: false, bpdu illegal length packets count: 0
 Autoedge swap-check: true
 Swap-delay time: 30
 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
```

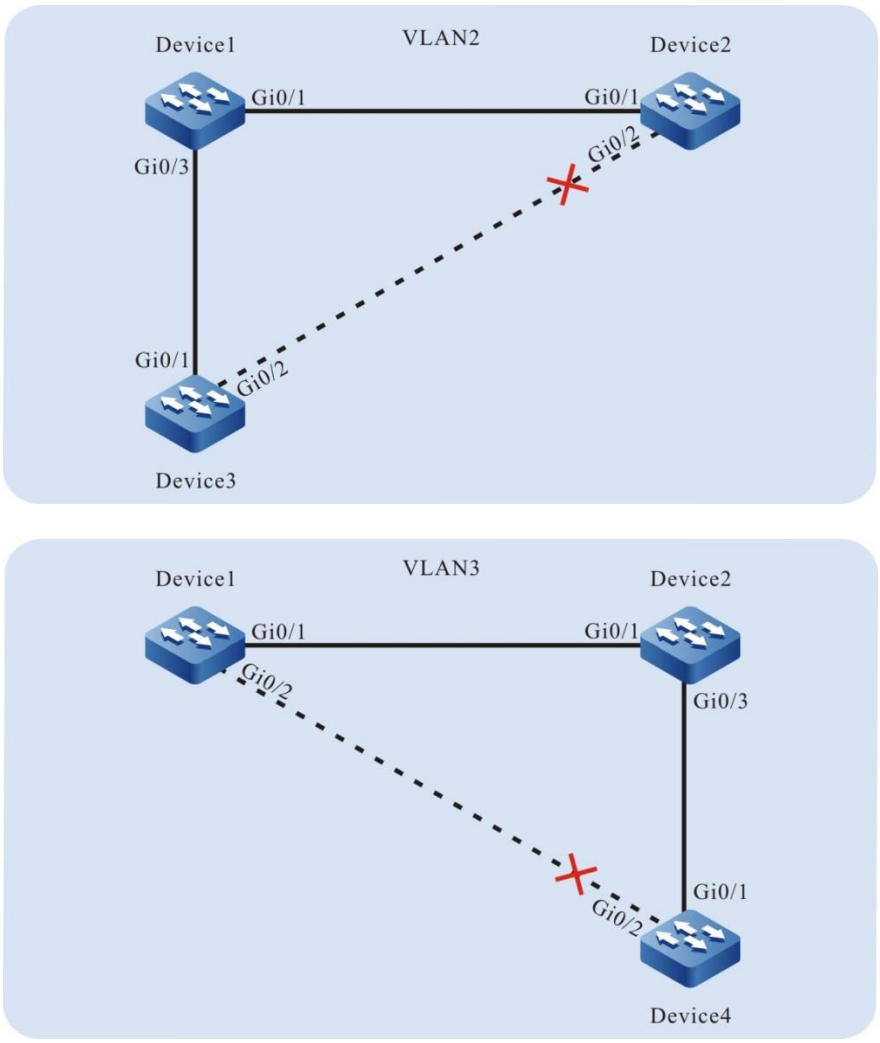
#On Device4, query the calculation result of all spanning tree instances. According to the result, port gigabitethernet0/1 of Device4 is blocked in instance 0, and port gigabitethernet0/2 is blocked in instance 2.

```
Device4#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00         vlans mapped:  1,4-4094
 Bridge              address 0101.7a58.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
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
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              Alte  DIS     20000   128.001 P2P
gi0/2              Root  FWD     20000   128.002 P2P
MST Instance 02        vlans mapped:  3
 Bridge ID           address 0101.7a58.dc0c priority 32770/32768
 Designated root     address 0101.7a54.5c96 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              Alte  DIS    20000   128.002 P2P
```

Based on the spanning tree calculation result of the four devices, the tree diagrams corresponding to MSTI 0 (mapped to VLAN4), MSTI 1 (mapped to VLAN2), and MSTI 2 (mapped to VLAN3) are obtained.





4.9.3.2 Apply MSTP Basic Functions in MLAG Environment

Network Requirements

- The four devices in the network are all in the same MST domain, and the bridge priority of the MLAG device is the highest.

Network Topology

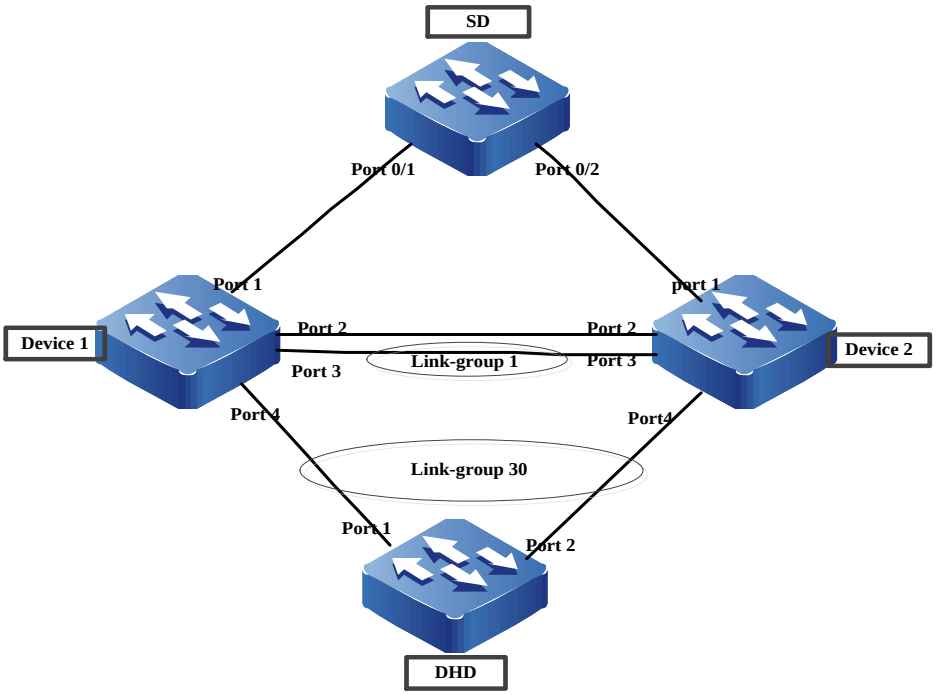


Figure 66 Networking for the application of MSTP in MLAG

Configuration Steps

Step 1: Add the interface to the aggregation group and add to the VLAN. (omitted)

Step 2: Configure the MLAG domain. (omitted)

Step 3: Configure the MST domain.

#Configure the MST domain on Device1, configure the domain name as admin and the revision level as 1 to activate the MST domain.

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst)#region-name admin
Device1(config-mst)#revision-level 1
Device1(config-mst)#active configuration pending
Device1(config-mst)#exit
```

Note

- The MST domain configuration of Device2, SD, and DHD is the same as Device1. (omitted)

View the information of each device spanning tree.

#Aggregation 1 on Device1 and Device2 is the interconnection port.

```
Device1#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1-4094
Bridge              address 0101.7a95.000b priority 0
Region root         address 0101.7a95.000b priority 0
Designated root     address 0101.7a95.000b priority 0
                    root: 0, rpc: 0, epc: 0, hop: 20
                    We are the root of the spanning tree
Operational  hello time 2, forward time 15, max age 20, message age 0
Configured   hello time 2, forward time 15, max age 20, max hops 20, hold count 10
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 2, interval 20s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:6, last change occured:118 weeks 5 days(71863322 seconds)
Interface          Role  Sts  Cost      Prio.Nbr  Type
------------------- ----- ---- --------- ---------- -------------------------
te0/1           Desg  FWD  20000     128.0036 P2P
link-agg1          Desg  FWD  1950      128.0193 P2P (MLAG peer-link)
link-agg30         Desg  FWD  19500     128.0222 P2P (MLAG 100)

Device2#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1-4094
Bridge              address 0101.7a95.000b priority 0
Region root         address 0101.7a95.000b priority 0
Designated root     address 0101.7a95.000b priority 0
                    root: 0, rpc: 0, epc: 0, hop: 20
                    We are the root of the spanning tree
Operational  hello time 2, forward time 15, max age 20, message age 0
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 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:7, last change occured:118 weeks 4 days(71776558 seconds)
Interface          Role  Sts  Cost      Prio.Nbr  Type
```

```
-------------------- ----- ---- --------- ---------- -------------------------
gi0/1            Desg  FWD  20000      128.0332 P2P
link-agg1          IRoot FWD  1950     128.0385 P2P (MLAG peer-link)
link-agg30          Desg  FWD  19500      128.0414 P2P (MLAG 100)
```

#SD connects the port of Device2 and the spanning tree calculation is block, and the mlag-group of DHD is Root.

```
SD#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1-4094
Bridge              address 0101.7a7a.3c10 priority 32768
Region root          address 0101.7a95.000b priority 0
Designated root       address 0101.7a95.000b priority 0
                    root: 32804, rpc: 20000, epc: 0, hop: 19
Operational  hello time 2, forward time 15, max age 20, message age 0
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 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 1
Topology Change Count:36, last change occured:118 weeks 5 days(71863036 seconds)
Interface          Role  Sts  Cost      Prio.Nbr  Type
-------------------- ----- ---- --------- ---------- -------------------------
gi0/1            Root  FWD  20000      128.0012 P2P
gi0/2            Alte  DIS  20000      128.0036 P2P

DHD#show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1-4094
Bridge              address 0101.7a6a.0148 priority 32768
Region root          address 0101.7a95.000b priority 0
Designated root       address 0101.7a95.000b priority 0
                    root: 33662, rpc: 18000, epc: 0, hop: 19
Operational  hello time 2, forward time 15, max age 20, message age 0
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 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 6
```

```
Topology Change Count:20, last change occured:118 weeks 5 days(71863409 seconds)
Interface        Role  Sts  Cost      Prio.Nbr  Type        -------------------- ----- ---- --
------- ---------- -------------------------
link-agg30       Root  FWD  18000     128.0894 P2P
```

Step 4: Modify the priority of the specified bridge of Device2, so that the blocked port of SA is calculated as 0/1.

```
Device2#conf t
Device2(config)#spanning-tree pseudo-information
Device2 (config-stp-pseudo)#mst instance 0 designated-priority 4096

SD# show spanning-tree
Spanning-tree enabled protocol mstp
MST Instance 00        vlans mapped: 1-4094
Bridge              address 0101.7a7a.3c10 priority 32768
Region root         address 0101.7a95.000b priority 0
Designated root     address 0101.7a95.000b priority 0
                    root: 32780, rpc: 20000, epc: 0, hop: 19
Operational  hello time 2, forward time 15, max age 20, message age 0
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 1, interval 4s, rxTcCnt 0, status:NORMAL
ARL flush: enabled
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 1
Topology Change Count:37, last change occured:118 weeks 5 days(71864200 seconds)
Interface        Role  Sts  Cost      Prio.Nbr  Type
-------------------- ----- ---- --------- ---------- -------------------------
gi0/1            Root  FWD  20000     128.0012 P2P
gi0/2            Alte  DIS  20000     128.0036 P2P
```

Step 5: Enable the BA function on the interconnection port of Device1 and Device2.

```
Device1(config)#interface link-aggregation 1
Device1(config-if-link-aggregation1)#spanning-tree bridge-assurance enable
Device2(config)#interface link-aggregation 1
Device2(config-if-link-aggregation1)#spanning-tree bridge-assurance enable
```

4.10Loopback Detection

4.10.1 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 Ethernet interfaces of a device, and loop on one Ethernet interface of a device. The two types of loops can be detected through loopback detection.

After the loopback detection function is enabled, the Ethernet interface sends loopback detection packets with an interval to check whether a loop exists in the network. When the Ethernet interface receives the loopback detection packet sent by the local device, it determines that a loop exists in the network. Then, the Ethernet interface is disabled to prevent the local loop from affecting the entire network.

4.10.2 Loopback Detection Function Configuration

Table 340 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 the Ethernet interface 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 the Ethernet interface.

4.10.2.1 Configure Basic Functions of Loopback Detection

Configuration Condition

None

Enable 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 the Ethernet interface takes effect only after the global loopback detection control switch is enabled.

Table 341 Enable 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 Loopback Detection Control Switch of Ethernet Interface or Aggregation Group

After the loopback detection function is enabled, the Ethernet interface sends loopback detection packets with an interval to check whether a loop exists in the network.

Table 342 Enabling the Loopback Detection Control Switch of the Ethernet interface or Aggregation Group

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L3/L2 Ethernet interface configuration mode.	interface *interface-name*	Either After entering the L2/L3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current Ethernet
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		interface. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enable the loopback detection control switch of the Ethernet interface or aggregation group.	loopback-detection enable	Mandatory. By default, the loopback detection control switch of the Ethernet interface or aggregation group is disabled.

Note

- In a loopback detection configuration task, you must enable the global loopback detection control switch before the loopback detection configuration on the Ethernet interface takes effect.

4.10.2.2 Configure Basic Parameters of Loopback Detection

Configuration Condition

None

Configure Sending Period of Loopback Detection Packets

In 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 343 Configure the sending period of the loopback detection packets

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2/L3 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 Ethernet interface. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	
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 Error-Disable Action of Ethernet Interface

If the Ethernet interface allows the Error-Disable action, the Ethernet interface is controlled. After a port detects a loop, it performs the Error-Disable action to close the Ethernet interface so as to eliminate the loop. If the Ethernet interface is not in the

controlled status, the Ethernet interface only prints loop prompt message instead of closing the Ethernet interface. In this case, the loop has not been eliminated.

Table 344 Configuring the Error-Disable Action on the Ethernet interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode.	interface *interface-name*	Either After entering the L2/L3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current Ethernet interface. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode.	interface link-aggregation *link-aggregation-id*	
Configure whether the Ethernet interface allows the Error-Disable function.	loopback-detection enable control	Mandatory. By default, after the Ethernet interface detects a loop, it performs the Error-Disable action.

4.10.2.3 Loopback Detection Monitoring and Maintaining

Table 345 Loopback Detection Monitoring and Maintaining

Command	Description
show loopback-detection [interface *interface-*	Displays the configuration information of all

Command	Description
name | interface link-aggregation *link-aggregation-id*]	Ethernet interfaces or a specified Ethernet interface in loopback detection.

4.10.3 Typical Configuration Example of Loopback Detection

4.10.3.1 Configure Remote Loopback Detection

Network Requirements

- Device1 and Device2 are directly connected, and Device2 has two L2 Ethernet interfaces which form a self-loop.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected Ethernet interfaces to eliminate the loop.

Network Topology

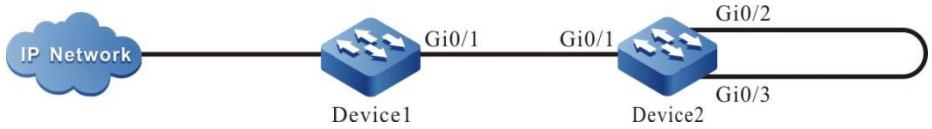


Figure 67 Networking for Configuring the Remote Loopback Detection Function

Configuration Steps of L2 Ethernet Interface

Step 1: Configure VLANs, and configure the link type of the L2 Ethernet interface.

#On Device1, create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of L2 Ethernet interface 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 L2 Ethernet interface gigabitethernet0/1, gigabitethernet0/2, and gigabitethernet0/3 to Trunk and allow the services of VLAN2 to pass. Configure the L2 Ethernet interface gigabitethernet0/2 and gigabitethernet0/3 to close the spanning tree.

```
Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
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 Device1, query the loopback detection status.

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
------------------- -------- ------- ------------ -------
gi0/1              DISABLE   30      NORMAL      TRUE
gi0/2              DISABLE   30      NORMAL      TRUE
```

#The L2 Ethernet interface gigabitethernet0/1 of Device1 enables the loopback detection function.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

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 L2 Ethernet interface gigabitethernet0/1 is closed, and the device outputs the following prompt information:

```
Jul 30 2014 03:30:30: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1, detected in vlan2 from gigabitethernet0/1
Jul 30 2014  03:30:30: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jul 30 2014 03:30:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#On Device1, query the status of L2 Ethernet interface gigabitethernet0/1, and you will find that the link status of the L2 Ethernet interface gigabitethernet0/1 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
```

Configuration Steps of L3 Ethernet Interface

Step 1: Configure VLAN, and configure the link type of the L2 Ethernet interface.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of L2 Ethernet interface gigabitethernet0/1, gigabitethernet0/2, and gigabitethernet0/3 to Trunk and allow the services of VLAN2 to pass. Configure the L2 Ethernet interface gigabitethernet0/2 and gigabitethernet0/3 to close the spanning tree.

```
Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#switchport trunk pvid vlan 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
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 Device1, view the loopback detection status.

```
Device1#show loopback-detection
 ----------------------------------------------------------
```

```
Global loopback-detection : ENABLE
-------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
-------------------- -------- ------- ------------ -------
gi0/1              DISABLE   30      NORMAL      TRUE
gi0/2              DISABLE   30      NORMAL      TRUE
```

#On Device1, configure the L2 Ethernet interface gigabitethernet0/1 as L3 Ethernet interface.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no switchport
```

#The L3 Ethernet interface gigabitethernet0/1 on Device1 enables the loopback detection function.

```
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

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 L2 Ethernet interface gigabitethernet0/1 is closed, and the device outputs the following prompt information:

```
Jul 31 2014 11:29:30: %LOOP-BACK-DETECTED : loop-back send packet on gigabitethernet0/1, detected from gigabitethernet0/1
Jul 31 2014 11:29:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
Jul 31 2014 11:29:30: %LINK-INTERFACE_DOWN-3: Interface gigabitethernet0/1, changed state to down.
Jul 31 2014 11:29:30: %LINK-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed state to down.
```

#On Device1, view the status of the L3 Ethernet interface gigabitethernet0/1 and you can see that the status of the L3 Ethernet interface changes to err-disabled.

```
Device1#show interface gigabitethernet 0/1 status err-disabled

Interface            Status       Reason
-------------------------------------------------------------
gi0/1              err-disabled   loopback-detect
```

4.10.3.2 Configure Local Loopback Detection

Network Requirements

- Device1 and Device2 form a loop through two links, and all L2 Ethernet interfaces in the loop is in one VLAN.
- On Device1, loopback detection has been enabled.
- After Device1 detects a loop, it closes the interconnected L2 Ethernet interfaces to eliminate the loop.

Network Topology

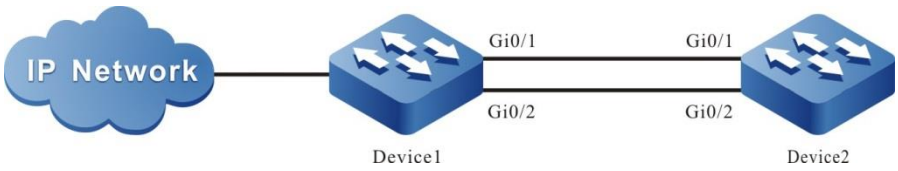


Figure 68 Networking for Configuring the Local Loopback Detection Function

Configuration Steps

Step 1: Configure VLANs, and configure the link type of the L2 Ethernet interface.

#On Device1, create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#On Device1, configure the link type of L2 Ethernet interface gigabitethernet0/1

and gigabitethernet0/2 to Trunk and allow the 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 L2 Ethernet interface gigabitethernet0/1 and gigabitethernet0/2 to Trunk, allow the services of VLAN2 to pass, and close the spanning tree.

```
Device2(config)# interface gigabitethernet 0/1-0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#no spanning-tree enable
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 Device1, query the loopback detection status.

```
Device1#show loopback-detection
------------------------------------------------------------
Global loopback-detection : ENABLE
------------------- -------- ------- ------------ -------
Interface          Loopback  Time(s) State       Control
------------------- -------- ------- ------------ -------
gi0/1              DISABLE   30      NORMAL      TRUE
gi0/2              DISABLE   30      NORMAL      TRUE
```

#The L2 Ethernet interface gigabitethernet0/1 on Device1 enables the loopback detection function.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

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 L2 Ethernet interface gigabitethernet0/1 is closed, and the device outputs the following prompt information:

```
Jul 30 2014 03:29:59: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1, detected in vlan2 from gigabitethernet0/2
Jul 30 2014  03:29:59: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jul 30 2014 03:29:59: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#On Device1, query the status of L2 Ethernet interface gigabitethernet0/1, and you will find that the link status of the L2 Ethernet interface gigabitethernet0/1 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
```

Note

- When gigabitethernet 0/1 or gigabitethernet 0/2 of Device1 is L3 Ethernet interface, there is no loop in the networking environment.

4.11 Error-Disable Management

4.11.1 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, Monitor Link, and fabric-failure.

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.

4.11.2 Error-Disable Management Function Configuration

Table 346 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.

4.11.2.1 Configure Error-Disable Basic Functions

Configuration Condition

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 347 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 | crc-error | dai | dhcp-snooping | monitor-link | torm-control | link-flap | l2pt |	Mandatory. By default, it is allowed that all the listed functions close a port and set the port to the Error-

Step	Command	Description
	mac-address-flapping | oam | port-security | loopback-detect | transceiver-power-high | transceiver-power-low }	Disabled status.

4.11.2.2 Configure Error-Disable Automatic Recovery

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 348 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 | crc-error | dai | dhcp-snooping | eips-udld | l2pt | link-flap | loopback-detect | mac-address-flapping | oam | port-security | storm-control | transceiver-power-high | transceiver-power-low | 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 349 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.

4.11.2.3 Error-Disable Management Monitoring and Maintaining

Table 350 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* | interface link-aggregation *link-aggregation-id* } status err-disabled	Displays the information about Error-Disabled status setting of a specified port or aggregation group.

4.11.3 Typical Configuration Example of Error-Disable Management

4.11.3.1 Combination of Error-Disable and Storm Suppression

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, you can disable the port via **Error-Disable**, and **Error-Disable** can re-enable the port according to the policy.

Network Topology

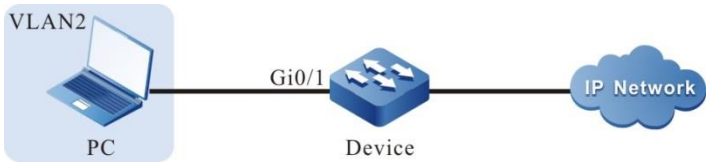


Figure 69 Networking for Combination of Error-Disable and Storm Suppression

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. During the storm, shut down the port.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control action shutdown
Device(config-if-gigabitethernet0/1)#storm-control broadcast pps 200
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           Enabled
loopback-detect     Disabled
oam                 Disabled
port-security       Disabled
storm-control       Enabled
crc-error           Disabled
ulfd                Disabled
transceiver-power-low  Disabled
transceiver-power-high Disabled
mac-address-flapping   Disabled
```

#When PC sends a large number of broadcast packets, port gigabitethernet0/1 is closed, and the following information is printed:

```
Nov 24 2014 15:37:13: %STORM_CONTROL-3: A storm detected on interface gigabitethernet0/1, ActionType:shutdown, StormType: broadcast storm
Nov 24 2014 15:37:13: %PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed state to down
.
```

#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 FD, 100M FD,1000M FD
    Link Delay      : No Delay
    Storm Control   : Unicast Pps 1500
    Storm Control   : Broadcast Pps 20
    Storm Control   : Multicast Pps 1500
    Storm Action    : Shutdown
    Port Type       : Nni
    Pvid            : 2
    Set Medium      : Copper
    Act Medium      : Copper
    Mac Address     : 0101.7a54.5ca5
```

#After 30s, enable the port gigabitethernet0/1and print the following prompt information.

```
Nov 24 2014 15:37:43: %PORTMGR-AUTO_RECOVERY-5: auto recovery timer expired on interface gigabitethernet0/1, module: STROM CONTROL ACTION.
Nov 24 2014 15:37:45: %PORTMGR-LINEPROTO_UP-5: Line protocol on interface gigabitethernet0/1, changed state to up.
```

#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 FD, 100M FD,1000M FD
Link Delay      : No Delay
Storm Control   : Unicast Pps 1500
Storm Control   : Broadcast Pps 20
Storm Control   : Multicast Pps 1500
Storm Action    : Shutdown
Port Type       : Nni
Pvid            : 2
Set Medium      : Copper
Act Medium      : Copper
Mac Address     : 0101.7a54.5ca5
```

4.12 GVRP

4.12.1 Overview

GVRP (GARP VLAN Registration Protocol), known as GARP VLAN registration protocol, is an application protocol defined by GARP. It dynamically maintains VLAN information in switches based on the protocol mechanism of GARP. All switches supporting GVRP feature can receive VLAN registration information from other switches and dynamically update local VLAN registration information, including current VLAN on the switch and which ports these VLANs contain, etc., and all switches supporting GVRP feature can spread local VLAN registration information to other switches, so as to make the VLAN configuration of all devices supporting GVRP features in the same switch network be consistent on in terms of interoperability. The VLAN registration information transmitted through GVRP includes not only the static VLAN information manually configured locally, but also the dynamic VLAN information from other switches. Note that the leave message of GVRP cannot delete the VLAN manually configured locally, that is to say, the priority of manually configured VLAN is higher than that of GVRP.

GVRP realizes the dynamic registration, maintenance and logout of VLAN port

member information. If the VLAN does not exist, the VLAN will be created dynamically; if the number of VLAN port members is 0, the VLAN will be deleted dynamically, that is, the port will be added to the VLAN or deleted from the VLAN dynamically, which also realizes the dynamic configuration of VLAN on the switch.

GVRP can dynamically configure VLANs, so it is not necessary to configure all VLANs of all devices, but only some devices, especially edge devices and some special VLANs. Other devices will be automatically configured through GVRP. Now the enterprise network is usually large and there are many VLANs. GVRP function greatly reduces the configuration work of administrators, and reduces the possibility of manual error. Moreover, when the network topology changes, the VLAN can be automatically configured to ensure the connectivity between VLANs.

4.12.2 GVRP Function Configuration

Table 351 GVRP function configuration list

Configuration Task	
Enable the GVRP function	Enable the GVRP function globally
Configure the GVRP port	Configure the port as trunk mode, and permitted VLAN
	Enable the GVRP function on the port
	Configure the GVRP mode of the port

4.12.2.1 Enable the GVRP Function

Configuration Condition

No

Enable the GVRP Function Globally

Enable the GVRP function globally.

Table 352 Enable the GVRP function globally

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enable the GVRP function globally	**gvrp enable**	Mandatory

4.12.2.2 Configure the GVRP Port

Configuration Condition

No

Configure the GVRP Port

Add the configuration on the port that needs to enable the GVRP function, including GVRP mode and the permitted VLAN.

Table 353 Enable the GVRP function of the port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter 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 Ethernet port. After entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the port as the trunk mode	switchport mode trunk	Mandatory
Configure the VLAN permitted by the port	switchport trunk allowed vlan all	Mandatory
Enable GVRP of the port	gvrp enable	Mandatory

4.13 MLAG

4.13.1 Overview

MLAG is a mechanism to realize cross-device link aggregation, which gathers one device and two other paired devices to form a dual-active system.

As a weak association horizontal virtualization technology, MLAG not only has the advantages of increasing bandwidth, providing link reliability and load sharing, but also has the following advantages:

- Higher reliability: MLAG improves link reliability from board level to device level. For common cross-board link aggregation, if one board fails, the whole aggregation link can still work normally; for MLAG cross-device link aggregation, even if one device fails, the whole aggregation link can still work normally.
- Simplify Networking: MLAG, as a horizontal virtualization technology, logically virtualizes two paired devices connected by dual homing into one device. MLAG provides a two-layer topology without loop and realizes redundant backup, so the access side does not need spanning tree protocol, which greatly simplifies the networking and configuration.
- Independent upgrade: two paired devices can be upgraded separately to ensure that one device can work normally, with little impact on the running business.
- The definitions of MLAG related concepts:
- MLAG (Multi-Chassis Link Aggregation Group) domain: consists of two MLAG pairing nodes, forming a dual active system.
- MLAG pairing node: in the MLAG pairing node, there is one node whose role is master and the other node whose role is slave.
- Peer link: the direct connection aggregation link between MLAG pairing

nodes, which is used to interact with MLAG protocol packets and transmit part of data traffic.

- Keep alive: keep alive detection between MLAG pairing nodes, which is carried out through L3 link. The function of MLAG is to judge whether the peer link is still alive after the peer link fails.
- PTS (Peer-Link Transport Server): Reliable packet transmission service based on peer link.
- DHD (Double-Homed Device): A device (or server) that is connected to the MLAG dual-active system via dual-homing. DHD itself may be a MLAG dual-active system.
- SD (Single-Homed Device): A device (or server) that is connected to the MLAG dual-active system via single-homing.
- MLAG-Port: Indicates the aggregation group across devices between DHD and MLAG dual-active system.
- MLAG Member Port: Indicates the member port of the aggregation group across devices between DHD and MLAG dual-active system.
- Orphan-Port: It refers to the single-homed access port on the MLAG pairing node, including the single-homed access aggregation group. The so-called orphan port belongs to MLAG VLAN, it may not belong to MLAG VLAN.
- MLAG-VLAN: The VLAN to which Peer-Link is added, all VLANs of the MLAG ports should be added to MLAG-VLAN
- non-MLAG-VLAN: The VLAN not containing Peer-Link, non-MLAG-VLAN does not contain the MLAG port
- MLAG-VLANIF: VLANIF interface corresponding to MLAG-VLAN
- non-MLAG-VLANIF: VLANIF interface corresponding to non-MLAG-VLA

- Unpaired: After the peer link port, if the keepalive is normal, it is considered that an unpaired fault has occurred, which will cause the MLAG port and MLAG-VLANIF on the slave node to be in the suspend state, making the uplink and downlink traffic be forwarded through the master node.
- Up-Delay: When the MLAG pairing node restarts or the peer link failure recovers, the MLAG port will delay for a period of time before being set to the UP state.
- Auto-Recovery: After a period of time, when the local MLAG node is judged to be completely disconnected from the peer MLAG node (the actual peer MLAG node may fail or still survive), the local MLAG node considers itself as the only node, becomes the master node, and forwards traffic.
- Dual-Master: If both peer link and keepalive fail, slave node judges to be completely disconnected with master node, slave node will be upgraded to master node, while the original master node still exists. At this time, there are two master nodes, namely dual-master. Traffic forwarding may be abnormal in dual-master state.
- Control protocol packet (also known as peering packet): the protocol packets interacted between MLAG nodes, used for node pairing, role election, etc., and sent and received through UDP.
- Data synchronization packet (also called sync packet): that is, the synchronization packet interacted between MLAG nodes, which is used to transmit control information, relay service protocol packet, synchronization service entry, etc. for each business. The sync packet is encapsulated with the PTS header information and is sent and received through TCP.
- Control VLAN: a L3 VLAN (interface VLAN) used to transmit PTS synchronous packets. Only peer link is allowed to join the VLAN, and other ports are not allowed to join the VLAN.

- Suspend: In this article, it refers to shutdown, which usually refers to the shutdown of MLAG aggregation group or MLAG-VLANIF interface.

4.13.2 MLAG Function Configuration

Table 354 MLAG function configuration list

Configuration Task	
Create one MLAG domain	Create one MLAG domain
Configure the MLAG parameters	Configure the delay time of auto recovery after node restarting
	Specify the local VLAN interface
	Configure the MLAG node ID
	Configure the priority of the MLAG node role
	Specify the peer IP address
	Configure the preemption mode
	Configure the MAC address of the MLAG system
	Configure the priority of the MLAG system
	Configure up state delay time and up state interval time
Configure the Keepalive parameters	Configure the source, source address and other parameters of the Keepalive packet
	Set the sending interval and receiving timeout of the Keepalive packet
	Set the Keepalive quiet period
Configure the Peer-Link	Configure the L2 aggregation interface as the Peer-link port
Configure the MLAG port	Configure the MLAG port
Configure the orphan port	Configure the orphan port of slave node to be set to shutdown state when peer link fails, but keepalive is normal

Note

- The MLAG function only supports the software learning, not supporting hardware learning.

4.13.2.1 Create One MLAG Domain

In the MLAG pairing nodes, the MLAG domain ID must be consistent.

Configuration Condition

Before creating the MLAG domain, first complete the following task:

- On the MLAG pairing nodes, there are other different MLAG domains

Create One MLAG Domain

Create one MLAG domain.

Table 355 Create one MLAG domain

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one MLAG domain	mlag domain *domain-id*	Mandatory By default, no MLAG domain is created, and the value range of domain ID is 1-255

4.13.2.2 Configure the MLAG Parameters

Configuration Condition

Before configuring the MLAG parameters, first complete the following task:

- Create one MLAG domain

Configure Auto Recovery Delay after Node Restarting

After the device starts, start the auto recovery timer with the configured auto recovery delay time. If no keepalive packet or peering packet is received until the timer expires, and the peer link is always down, then the peer node is considered to be nonexistent and the node becomes master.

Table 356 Configure the auto recovery time after the node restarts

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the auto recovery time after the node restarts	auto-recovery reload-delay *delay_value*	Optional By default, the auto recovery delay is 240s, and time range of the auto recovery delay is 240-3600s.

Configure MLAG Node ID

In the same MLAG domain, MLAG node IDs are different and unique.

Table 357 Configure the MLAG node ID

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the MLAG node ID	node id *id-number*	Mandatory By default, do not configure the MLAG node ID, and the ID range of the MLAG node is 1 and 2.

Configure the Priority of MLAG Node Role

Node role priority is used to select the master-slave role between two nodes in the same MLAG domain. The smaller the value, the higher the priority, and the one with

higher priority becomes the master device. If the node priority is the same, compare the bridge MAC addresses of the two devices, and the one with smaller bridge MAC address becomes the master device.

Table 358 Configure the priority of the MLAG node role

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the priority of the MLAG node role	node role-priority *priority-value*	Optional By default, MLAG node priority is 100, and MLAG node priority ranges from 1 to 254

Configure the Preempt Mode

If the preemption mode is configured, the previous role of the node will be ignored when the master-slave role is elected, and the role of the node will be determined based on the comparison result of node priority and bridge MAC: The lower the priority value of the node is, the higher the priority is, the node with the higher priority becomes the master device; if the node priority is the same, compare the bridge MAC addresses of the two devices, and the smaller the bridge MAC address becomes the master device.

Table 359 Configure the preempt mode

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the preempt mode	role preempt	Optional By default, do not configure the preempt mode.

Configure the MAC Address of the MLAG System

To enable the access device to treat two nodes in the MLAG domain as one device, the MAC addresses of the MLAG system of the two nodes must be the same.

Table 360 Configure the MAC address of the MLAG system

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the MAC address of the MLAG system	system-mac *mac_address*	Optional By default, the MAC address of MLAG system is not configured. The MAC addresses of MLAG system of the two nodes is automatically generated according to the domain ID and remain the same.

Configure the MLAG System Priority

To enable the access device to treat two nodes in the MLAG domain as one device, the MAC addresses of the MLAG system of the two nodes must be the same.

Table 361 Configure the priority of the MLAG system

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the priority of the MLAG system	system-priority *priority_value*	Optional By default, the priority of the MLAG system is 32768, and the priority range of the MLAG

		system is 1-65535.

Configure the Delay of UP State and Interval of UP State

When the device joins the MLAG domain as a slave node, the MLAG interface will be set to the up state only after the delay time of the up state. During the delay of the up state, MAC address table, ARP table and other information will be synchronized, so if there are many entries, the timer can be extended appropriately to avoid packet loss.

Table 362 Configure the delay time of the UP state and the interval of the UP state

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the delay time of the UP state and the interval of the UP state	up-delay *delay_seconds* [interval *interval_mseconds*]	Optional By default, the delay time of the up state is 90 seconds, the interval time of the up state is 1000 milliseconds, the delay time range of the up state is 1-3600, and the interval time of the up state is 1-300000 milliseconds

Configure MLAG Graceful Restart

After enabling graceful restart, the node will notify the peer node to extend the time of the control protocol alive and keepalive, so as to avoid traffic interruption caused by timeout of the peer node when the MLAG of the node is restarted. It is recommended that this command be configured only before MLAG restart. Normally, configuring this command will make the peer node insensitive to network changes.

By default, graceful restart of mlag is not enabled.

Table 363 Configure MLAG graceful restart

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the graceful restart of MLAG, and the time of keeping the peer control protocol alive and keepalive alive after restart	mlag graceful-restart [holding-time seconds]	Optional By default, the keepalive time is 300s, and the time range of the keepalive delay is 200-20000s.

Configure Reserved Interface

The VLAN interface used to configure slave nodes is not set to shutdown state when peer link fails, but keepalive is normal.

By default, reserved interfaces are not configured.

Table 364 Configure the reserved interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the reserved interface	mlag unpaired reserved	Optional The VLAN corresponding to the interface needs to be MLAG-VLAN. The non-MLAG-VLANIF interface does not need to configure this command, because this kind of interface will not be set to shutdown state

4.13.2.3 Configure the Keepalive Parameters

Configuration Condition

Before configuring the Keepalive parameters, first complete the following task:

- Create one MLAG domain

Configure Source, Destination Address and Other Parameters of Keepalive Packet

To establish the MLAG system correctly, the source and destination addresses of keepalive packet must be configured, and the L3 layer between two nodes is reachable.

The VLAN corresponding to the L3 interface to which the source IP address of the keepalive packet belongs cannot be included in the VLAN where the peer link interface is located.

Table 365 Configure the source, destination address and other parameters of the Keepalive packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the source, destination addresses and other parameters of the Keepalive packet	keepalive ip destination *ipv4_address* source *ipv4_address* [udp-port *udp-number*] [vrf *vrf_name*]	Mandatory By default, the udp-port is 53910, VRF name is global, udp-port range is 1-65535, and VRF name supports up to 31 characters.

Configure Sending Interval and Receiving Timeout of the Keepalive Packet

When receiving the previous keepalive packet or when starting to listen, start the receiving timeout timer with the receiving timeout. If the timer does not receive the next keepalive packet before the expiration, it is considered as LOST.

Table 366Configure the sending interval and receiving timeout of the Keepalive packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain	mlag domain *domain-id*	-

configuration mode.		
Configure the sending interval and receiving timeout of the Keepalive packet	keepalive interval *mseconds* [timeout *seconds*]	Optional By default, the transmission interval of keepalive packet is 1000ms, the receiving timeout of keepalive packet is 6s, the sending interval range of keepalive packet is 100-10000, and the receiving timeout of keepalive packet is 1-20s

Configure the Quiet Time of the Keepalive Packet

After the peer-link is down, the slave node enters the quiet period. The keepalive packets received during the quiet period will be ignored and will not be processed. The keepalive packets received after the quiet period will be processed. The quiet period is to wait for the keepalive packets on the link to be received and sent completely, so as to prevent false detection due to packet delay.

Table 367Configure the quiet time of the Keepalive packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the MLAG domain configuration mode.	mlag domain *domain-id*	-
Configure the quiet time of the Keepalive packet	keepalive quiet-time *mseconds*	Optional By default, the quiet period of the Keepalive packet is 3000ms, and the value range of the quiet time is 1-15000ms.

4.13.2.4 Configure the Peer-link Link

Configuration Condition

Before configuring the Peer-link, first complete the following task:

- Create one MLAG domain

Configure the L2 Aggregation Interface as Peer-Link Port

Peer-link is a direct-connected link aggregation link between two MLAG devices, which is used to interact with MLAG protocol packets and transmit part of data traffic.

Table 368 Configure the L2 aggregation interface as Peer-Link port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 aggregation interface configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the L2 aggregation interface as Peer-Link port	mlag peer-link	Mandatory By default, do not configure the Peer-Link port.

4.13.2.5 Configure the MLAG Port

Configuration Condition

Before configuring the MLAG port, first complete the following task:

- Create one MLAG domain

Configure the MLAG Port

To provide reliability and avoid loops in the configuration process, on two MLAG pairing nodes, configure the aggregation group docking with the same convergence group on DHD as the same MLAG port ID to form a cross-device link aggregation group.

Table 369 Configure the MLAG port

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 aggregation interface configuration mode	interface link-aggregation *link-aggregation-id*	-
Configure the MLAG port	mlag group *mlag-id*	Mandatory By default, do not configure the MLAG port, and the ID of the MLAG port is 1-1000.

Note

- It is suggested to configure the link aggregation group as the dynamic aggregation group.

4.13.2.6 Configure the Orphan Port

Configuration Condition

Before configuring the Orphan port, first complete the following task:

Create one MLAG domain

Configure Orphan Port of SLAVE Node as Shutdown when Peer-Link fails, but Keepalive Is Normal

By default, when peer link fails, but keepalive is normal, all MLAG ports of the slave node will be set to shutdown state, but orphan ports will not be set to shutdown state. If you want to set some orphan ports to shutdown state, you need to configure this command for these orphan ports

Table 370 Configure the orphan port of the slave node to shutdown when Peer-link fails, but Keepalive is normal

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
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 the L2 aggregation interface configuration mode, the subsequent configuration takes effect only on the aggregation group.
Enter the L2 aggregation interface configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the orphan port of the slave node to shutdown when Peer-link fails, but Keepalive is normal	mlag unpaired orphan-port suspend	Optional By default, do not configure the command.

4.13.2.7 MLAG Monitoring and Maintaining

Table 371 MLAG Monitoring and Maintaining

Command	Description
clear mlag packet keepalive statistics [tx | rx]	Clear MLAG keepalive packet statistics
clear mlag packet peering statistics [tx | rx]	Clear MLAG peering packet statistics
clear mlag packet statistics pts [application *app-id*] [tx | rx]	Clear MLAG PTS packet statistics
clear mlag packet sync statistics [tx | rx]	Clear MLAG Sync packet statistics
show mlag pts application	Display the all service information of MLAG
show mlag brief	Display the MLAG brief information
show mlag group [*mlag-id*]	Display the MLAG aggregation group information
show mlag keepalive	Display the MLAG Keepalive information
show mlag node	Display the information of the MLAG node

Command	Description
show mlag packet pts [application [*app-id*]] statistics	Display the statistics information of the received and sent PTS packets of all MLAG services or specified MLAG service
show mlag packet keepalive statistics	Display the statistics information of the MLAG Keepalive packet
show mlag packet peering statistics	Display the statistics information of MLAG pairing packets
show mlag packet sync statistics	Display the statistics information of the MLAG synchronization packets
show mlag suspend	Display the Suspended interfaces
show mlag up-delay	Display the interfaces waiting for timeout of the up-delay timer

4.13.3 MLAG Typical Configuration Example

4.13.3.1 Configure MLAG Basic Functions

Network Requirements

All devices are in one L2 network.

Network Topology

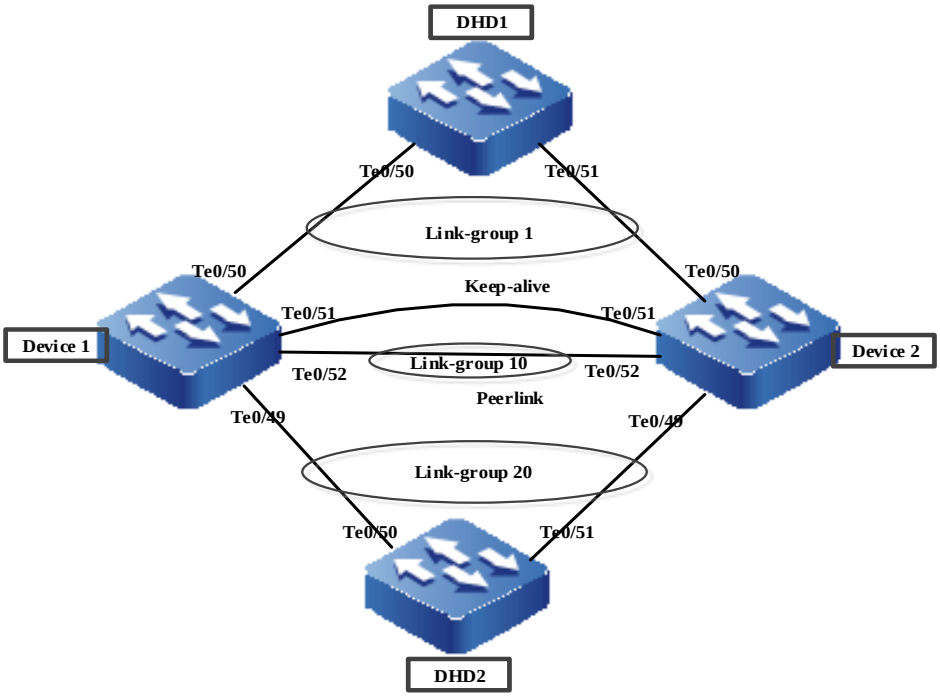


Figure 70 Configure MLAG basic functions

Configuration Steps

Step1: Add the interface to the aggregation group.

#Configure Device1, add the interface to the peerlink aggregation group, and add peerlink aggregation to the VLAN

And configure the keepalive port to join the VLAN.

```
Device1#configure terminal
Device1(config)#vlan 2-4093
Please wait ……
Done.
Device1(config)# link-aggregation 10 mode lacp
Device1(config)# interface tengigabitethernet 0/52
Device1(config-if-tengigabitethernet0/52)# link-aggregation 10 active
Device1(config-if-port3)#exit
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)# switchport mode trunk
Device1(config-link-aggregation10)# switchport trunk allowed vlan add 2-4093
Device1(config-link-aggregation10)# no switchport trunk allowed vlan 1
Device1(config-link-aggregation10)# switchport trunk pvid vlan 2
Device1(config-link-aggregation10)#exit
Device1(config)# interface tengigabitethernet 0/51
Device1(config-if- tengigabitethernet 0/51)# switchport access vlan 4094
```

```
Device1(config-if- tengigabitethernet 0/51)#exit
Device1(config)# link-aggregation 1 mode lacp
Device1(config)# interface tengigabitethernet 0/50
Device1(config-if- tengigabitethernet 0/50)# link-aggregation 10 active
Device1(config-if- tengigabitethernet 0/50)#exit
Device1(config)# link-aggregation 20 mode lacp
Device1(config)# interface tengigabitethernet 0/49
Device1(config-if- tengigabitethernet 0/49)# link-aggregation 20 active
Device1(config-if- tengigabitethernet 0/49)#exit
Device1(config)# interface link-aggregation 1
Device1(config-link-aggregation1)# switchport mode trunk
Device1(config-link-aggregation1)# switchport trunk allowed vlan add 2-4093
Device1(config-link-aggregation1)# no switchport trunk allowed vlan 1
Device1(config-link-aggregation1)# switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
Device1(config)# interface link-aggregation 20
Device1(config-link-aggregation20)# switchport mode trunk
Device1(config-link-aggregation20)# switchport trunk allowed vlan add 2-4093
Device1(config-link-aggregation20)# no switchport trunk allowed vlan 1
Device1(config-link-aggregation20)# switchport trunk pvid vlan 2
Device1(config-link-aggregation20)#exit
```

#Configure Device2, add the interface to the peerlink aggregation group, and add peerlink aggregation to the VLAN

```
And configure the keepalive port to join the VLAN.
Device2#configure terminal
Device2 (config)#vlan 2-4093
Please wait ……
Done.
Device2 (config)# link-aggregation 10 mode lacp
Device2 (config)# interface tengigabitethernet 0/52
Device2 (config-if-tengigabitethernet0/52)# link-aggregation 10 active
Device2 (config-if-tengigabitethernet0/52)#exit
Device2 (config)# interface link-aggregation 10
Device2 (config-link-aggregation10)# switchport mode trunk
Device2 (config-link-aggregation10)# switchport trunk allowed vlan add 2-4093
Device2 (config-link-aggregation10)# no switchport trunk allowed vlan 1
Device2 (config-link-aggregation10)# switchport trunk pvid vlan 2
Device2 (config-link-aggregation10)#exit
Device2 (config)# interface tengigabitethernet 0/51
Device2 (config-if-tengigabitethernet0/51)# switchport access vlan 4094
Device2 (config-if-tengigabitethernet0/51)#exit
Device2(config)# link-aggregation 1 mode lacp
```

```
Device2(config)# interface tengigabitethernet 0/50
Device2(config-if- tengigabitethernet 0/50)# link-aggregation 10 active
Device2(config-if- tengigabitethernet 0/50)#exit
Device2(config)# link-aggregation 20 mode lacp
Device2(config)# interface tengigabitethernet 0/49
Device2(config-if- tengigabitethernet 0/49)# link-aggregation 20 active
Device2(config-if- tengigabitethernet 0/49)#exit
Device2(config)# interface link-aggregation 1
Device2(config-link-aggregation1)# switchport mode trunk
Device2(config-link-aggregation1)# switchport trunk allowed vlan add 2-4093
Device2(config-link-aggregation1)# no switchport trunk allowed vlan 1
Device2(config-link-aggregation1)# switchport trunk pvid vlan 2
Device2(config-link-aggregation1)#exit
Device2(config)# interface link-aggregation 20
Device2(config-link-aggregation20)# switchport mode trunk
Device2(config-link-aggregation20)# switchport trunk allowed vlan add 2-4093
Device2(config-link-aggregation20)# no switchport trunk allowed vlan 1
Device2(config-link-aggregation20)# switchport trunk pvid vlan 2
Device2(config-link-aggregation20)#exit
```

Step2: Configure the MLAG domain.

#Configure Device1, and configure the MLAG domain instance.

```
Device1#configure terminal
Device1(config)#mlag domain 1
Device1(config-mlag-domain)#node id 1
Device1(config-mlag-domain)#keepalive ip destination 30.0.0.10 source 30.0.0.20
Device1(config-mlag-domain)#exit
```

##Configure Device2, and configure the MLAG domain instance.

```
Device2#configure terminal
Device2(config)#mlag domain 1
Device2(config-mlag-domain)#node id 2
Device2(config-mlag-domain)#keepalive ip destination 30.0.0.20 source 30.0.0.10
Device2(config-mlag-domain)#exit
```

Note

- The domain IDs of two MLAG nodes should be the same.
- The node IDs of two MLAG nodes cannot be the same.

Step3: Configure keepalive ip interface.

#Configure Device1, and configure keepalive ip interface.

```
Device1(config)#interface vlan 4094
Device1(config-if-vlan4094)#ip address  30.0.0.10 24
Device1(config-if-vlan4094)#exit
Device1(config)#
```

#Configure Device2, and configure keepalive ip interface.

```
Device2(config)#interface vlan 4094
Device2(config-if-vlan4094)#ip address  30.0.0.20 24
Device2(config-if-vlan4094)#exit
Device2(config)#
```

Note

- The keepalive link is directly connected through the vlan if interface of the Mlag node. If the device has enabled the spanning tree protocol, pay attention to the division of instances;

Step4: Configure mlag group and peer-link group.

#Configure Device1, and configure mlag group and peer-link group.

```
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mlag group 1
Device1(config-link-aggregation1)#exit
Device1(config)# interface link-aggregation 20
Device1(config-link-aggregation20)#mlag group 20
Device1(config-link-aggregation20)#exit
Device1(config)# interface link-aggregation 10
Device1(config-link-aggregation10)#mlag peer-link
Device1(config-link-aggregation10)#exit
```

#Configure Device2, and configure mlag group and peer-link group.

```
Device2(config)# interface link-aggregation 1
Device2(config-link-aggregation1)#mlag group 1
Device2(config-link-aggregation1)#exit
Device2(config)# interface link-aggregation 20
Device2(config-link-aggregation20)#mlag group 20
Device2(config-link-aggregation20)#exit
Device2(config)# interface link-aggregation 10
```

```
Device2(config-link-aggregation10)#mlag peer-link
Device2(config-link-aggregation10)#exit
```

Note

- VLANs allowed by mlag group should be included in VLANs allowed by peerlink group, which can be adjusted according to the actual situation

#Query the MLAG information on Device1.

```
Device1#sho mlag brief
MLAG domain id       : 1
Role FSM status      : SLAVE
Peering FSM status   : ESTABLISHED
Keepalive FSM status  : ALIVE
PTS Service          : ON
Up-delay             : 90sec
Graceful-restart     : Disabled
Number of mlags configured : 2

------------------------------------------------------
Peer-Link          Link-status Data-status Active-vlans
------------------- ----------- ----------- --------
link-aggregation 10  LINKUP     UP        2-4093

------------------------------------------------------
Node    ID   Role    System-MAC     System-Priority
------- ---- ------- -------------- ----------------
Self    1    SLAVE   0101.7a95.000b  32768
Remote  2    MASTER  0101.7a95.000b  32768
Device1#
Device1#show  mlag group
Number of mlags configured : 2

mlag-id: 1 (link-aggregation1)
--Link status: LINKUP
--Data status: UP
--Active mlag vlans: 2-4093
--Redirect FSM state: UNREDIRECT
--Isolate FSM state: ISOLATE
--Block FSM state: UNBLOCK
--Remote interface: link-aggregation 1
--Remote link status: LINKUP
--Remote data status: UP
```

```
mlag-id: 20 (link-aggregation 20)
--Link status: LINKUP
--Data status: UP
--Active mlag vlans: 2-4093
--Redirect FSM state: INVALID
--Isolate FSM state: ISOLATE
--Block FSM state: UNBLOCK
--Remote interface: link-aggregation 20
--Remote link status: LINKUP
--Remote data status: UP
```

4.14 VLAN Isolation

4.14.1 Overview

In the user access network, in order to achieve the isolation between different user groups, different user groups need to be divided into different VLANs. If the users in the same user group want to realize the isolation between users, the port isolation technology can be used, but this technology requires the administrator to clearly know the port location of the user access network, which makes the configuration and management maintenance inconvenient. VLAN isolation technology solves this problem skillfully. Administrators only need to configure VLAN isolation for the VLAN of the user group, and each user in the user group will be isolated from each other. By configuring the uplink port of VLAN isolation, users in the user group can access the public network through the uplink port. This technology provides a more secure and flexible scheme for networking.

4.14.2 VLAN Isolation Function Configuration

Table 372 VLAN global function configuration list

Configuration Task	
Configure the VLAN isolation	Enable the VLAN isolation function
	Configure the uplink port of the VLAN isolation

4.14.2.1 Configure VLAN Isolation

Configuration Condition

None

Enable VLAN Isolation Function

By enabling VLAN isolation function, the member ports in VLAN can be isolated from each other.

Table 373 Enable the global VLAN isolation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	-
Enable the VLAN isolation function	vlanIsolat enable	Mandatory By default, do not enable the VLAN isolation function.

Configure Uplink Port of VLAN Isolation

After configuring the uplink port of the VLAN isolation, the downlink ports in the VLAN are still isolated from each other, but the uplink ports and uplink ports, and the uplink ports and downlink ports can communicate with each other.

Table 374 Configure the uplink port of VLAN global isolation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure the uplink port of VLAN global isolation	vlanIsolate uplink-port vlan *vlan-id*	Mandatory By default, do not configure the uplink port of the VLAN isolation.

Note

- After the global VLAN isolation function is disabled, the configured uplink port of the VLAN isolation is automatically cancelled, VLAN isolation is enabled, and all ports in VLAN are downlink ports by default.

4.14.2.2 VLAN Isolation Monitoring and Maintaining

Table 375 Monitoring and maintaining of VLAN global isolation

Command	Description
show vlan-isolate([vlan *vlan-id*])	Display the VLAN isolation information

5 IP Protocol and Services

5.1 ARP

5.1.1 Overview

Address Resolution Protocol (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.

5.1.2 ARP Function Configuration

Table 376 ARP Function List

Configuration Tasks	
Configure basic functions of ARP.	Configure static ARP
	Configure the local ARP advertising
	Configure the maximum number of dynamic ARP entries.
	Configure the dynamic ARP aging time.
	Enable the dynamic APP learning function
	Enable ARP dynamic passive learning function
	Configure the ARP receive queue depth.
	Configure ARP proxy.
	Enable the ARP fast response function

5.1.2.1 Configure Basic Functions of ARP

Configuration Condition

None

Configure a Static ARP Entry

Configuring static ARP means that a user manually specifies the mapping between IP addresses and MAC addresses.

Table 377 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]] [vlan *vlan-id* {{ interface *if-name*} | { link-aggregation *link-aggregation-id* }}]	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.
- When the static ARP is bound to the specific port or aggregation group, the static ARP just takes effect on the port or aggregation group.

Configure Local ARP Advertising

ARP request packet is the broadcast packet. When there are lots of ARP requests in the network, it is easy to generate the broadcast storm on the network and as a result, the normal ARP request packets may be flooded and cannot learn ARP. In the case, we can configure the local ARP advertising function to reduce the ARP requests and the possibility of the broadcast storm.

Table 378 Configure the Local ARP Advertising

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure local ARP advertising	arp local-announce enable	Mandatory
Configure the interval of the local ARP advertising	arp local-announce interval *seconds*	Optional By default, it is 10s.
Configure the rate of the local ARP advertising	arp local-announce rate *speed*	Optional By default, it is one packet every second.

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 379 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 5000.

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 380 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 learned Function

By default, a device can perform the dynamic APR passive learning. To prevent dynamic learned ARP from occupying too many system resources, you can disable the dynamic ARP passive learning function. After dynamic ARP passive 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 actively requests for the MAC address of a peer device.

Table 381 Enable the dynamic ARP passive learning function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the dynamic ARP passive learning function.	arp learn-active	Mandatory By default, enable the dynamic ARP passive learning function.

Enable Dynamic ARP Learning

By default, the interface can perform the dynamic ARP learning. To get more reliable security, the user can disable the dynamic ARP learning function of the interface and use the static ARP, so as to prevent the ARP spoofing.

Table 382 Enabling Dynamic ARP Learning

Step	Command	Description
Enter the interface configuration mode.	configure terminal	-

Step	Command	Description
Enable dynamic ARP learning.	arp learn-active	Mandatory. By default, dynamic ARP learning is enabled.

Configure ARP Receive Queue Length

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 length based on the network ARP emergency.

Table 383 Configure the ARP receive queue length

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the ARP receive queue length	arp queue-length *length*	Mandatory The queue length 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 384 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.

Configure ARP Fast Response

By default, after receiving the ARP request packet, the device will go to the control board for learning and response. After the ARP quick response function is enabled, the ARP packet can be answered quickly in the LPU.

Table 385 Configure ARP fast response

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure ARP fast response	arp fast-response	Mandatory By default, the global ARP fast response function is disabled.

5.1.2.2 ARP Monitoring and Maintaining

Table 386 ARP Monitoring and Maintaining

Command	Description
show arp [vrf *vrf-name*]	Display the ARP table.
show arp attack-detection	Display the information about the host which has been suspected of initiating ARP attacks.
show arp statistic	Display the ARP statistics information

5.1.3 ARP Typical Configuration Example

5.1.3.1 Configure ARP Proxy

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 0101.7a13.0102.
- Through the ARP proxy of Device, PC1 can successfully ping PC2, and PC1 can learn the MAC address of PC2.

Network Topology

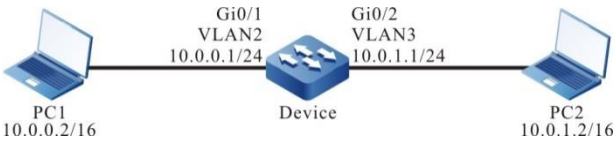


Figure 71 Networking for Configuring ARP Proxy

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      -       0101.7a13.0102  ARPA   vlan2       ---
Internet  10.0.0.2      1       B8AC.6F2D.4498  ARPA   vlan2       gigabitethernet0/1
Internet  10.0.1.1      -       0101.7a13.0103  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.

5.1.3.2 Configure a Static ARP Entry

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

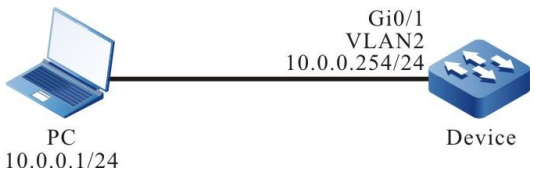


Figure 72 Networking for Configuring a Static ARP Entry

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  -      0101.7a13.0102  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.

5.2 IP Basics

5.2.1 Overview

The Internet Protocol (IP) is based on data packets. It is used in data exchange between computer networks. The protocols that are supported by the device include: IP, Internet Control Message Protocol (ICMP), Transfer 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.

5.2.2 IP Basic Function Configuration

Table 387 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.
	Enable IP routing cache.
Configure basic functions of the ICMP protocol.	Enable global ICMP redirection.
	Enable global ICMP redirection.
	Enable ICMP destination unreachable.
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.

Configuration Tasks	
	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.

5.2.2.1 Configure an IP Address

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 388 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	240.0.0.0-255.255.255.254	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, 172.16.0.0-172.31.255.255, 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 Condition

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 389 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*	Mandatory.

Step	Command	Description
	{ *network-mask* | *mask-len* } [secondary]	

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 390 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*	-
Configure an unnumbered IP address for an	ip unnumbered *reference-interface*	Mandatory.

Step	Command	Description
interface.		

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.

5.2.2.2 Configure Basic Functions of the IP Protocol

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 Condition

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 391 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 392 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 393 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 394 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 395 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.

5.2.2.3 Configure Basic Functions of the ICMP Protocol

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 Condition

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 396 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 disabled.

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 397 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. 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 Network Unreachable

After the device receives an IP packet, if an unreachable error occurs in the destination network, drop the packet and send the unreachable error packet of the ICMP destination network to the source.

- For the forwarded IP packet, if searching for the route failed, send the

"Network unreachable" ICMP error packet back to the source end.

Table 398 Enable ICMP destination network unreachable

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable ICMP destination network unreachable	ip network unreachables reply	Optional By default, do not enable ICMP destination network unreachable.

Enable ICMP Destination Unreachable

After a device receives IP data packets, 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 399 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 Source Interface

ICMP error packet supports response using loopback interface address, that is, configure loopback interface and specify this interface address as ICMP packet source address, so that the device sending ICMP error packet can be quickly determined through ICMP packet source address in complex network. For ICMPv6 type error packet, the source address of the packet is also specified through this command.

Table 400 Configure ICMP source interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure ICMP source interface	ip icmp source-interface *interface-name*	Mandatory By default, do not configure the ICMP source interface.

5.2.2.4 Configure Basic Functions of the TCP Protocol

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 Condition

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 401 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 402 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 403 Configuring the Maximum Number of TCP Retransmissions

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
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 404 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 405 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 406 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 407 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 408 Configuring the Maximum Number of TCP Keep-Alive Times

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the maximum	ip tcp keep-count *keep-count*	Mandatory.

Step	Command	Description
number of TCP keep-alive times.		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 409 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 410 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.

5.2.2.5 Configure TCP Protocol Anti-attack Function

If the TCP server receives lots of SYN packets, but the peer does not respond to

the SYN+ACK response of the server, lots of server memory is consumed and the half-connection queue of the server is occupied. As a result, the TCP server cannot provide the normal request service. As for the attack, you can configure the TCP anti-attack function.

Configuration Condition

None

Enable TCP syncache Function

When receiving the SYN packet, do not distribute TCB at once, but first return one SYN ACK packet, and save the half-connection information in the private HASH table (Cache) until receiving the correct response ACK packet, and then distribute TCB.

Table 411 Enable the TCP syncache function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the TCP syncache function	ip tcp syncache	Mandatory By default, the function is disabled.

Enable TCP syncookies Function

The function does not use any stored resources, but adopts one special algorithm to generate Sequence Number. The algorithm considers the peer IP, port, the own IP, and port fixed information, as well as other fixed information, such as MSS and time. After receiving the ACK packet of the peer, re-calculate and view whether it is the same as Sequence Number-1 in the response packet of the peer, so as to decide whether to distribute the TCB resources.

Table 412 Enable the TCP syncookies function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the TCP syncookies function	ip tcp syncookies	Mandatory By default, the function is

		disabled.

5.2.2.6 Configure Basic Functions of the UDP Protocol

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 Condition

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 413 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 414 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 415 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 416 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 417 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.

5.2.2.7 IP Basics Monitoring and Maintaining

Table 418 IP Basics Monitoring and Maintaining

Command	Description
clear ip icmpstat	Clears ICMP protocol statistics.
clear ip statistics	Clears IP protocol statistics.
clear ip tcp syncache statistics	Clears the syncache statistics information of the TCP protocol
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.
show ip sockets	Displays the Socket details.
show ip statistics	Displays IP protocol statistics.
show ip tcpstat	Displays TCP protocol statistics.
show ip tcp syncache statistics	Displays the TCP syncache statistics information

Command	Description
show ip udpstat	Displays UDP protocol statistics.
show ip tcp syncache detail	Displays the syncache entry information of the TCP protocol
show tcp tcb [detail]	Displays TCP protocol control block details.

5.3 DHCP

5.3.1 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 client, 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.

5.3.2 DHCP Function Configuration

Table 419 DHCP Function List

Configuration Tasks	
Configure a DHCP address pool	Create a DHCP address pool and specify the VRF attributes
	Configure an IP address range.
	Configure a DNS server address.
	Configure the default route.
	Configure the domain-name
	Configure the lease of an IP address.
	Bind an IP address and a MAC address.

	Configure the bootfile field
	Configure the next-server field
	Configure user-defined options.
	Configure the specified manufacturer address pool.
Configure other parameters of a DHCP server.	Configure the DHCP server
	Configure the reserved IP address range
	Configure DHCP ping detection parameters.
	Configure the DHCP data log function
	Configure lease update of DHCP address pool
	Configure DHCP to support unicast reply
Configure the functions of a DHCP client.	Configure a DHCP client.
	Configure the manufacturer ID
	Configure the DHCP route distance
	Configure the DHCP 60 option function
	Configure the DHCP client not to request for the default route option
Configure the DHCP relay function	Configure the interface DHCP relay.
	Configure the Option82 function.
	Configure the source address of the interface DHCP relay packet
	Configure the DHCP server address

5.3.2.1 Configure a DHCP Address Pool

Configuration Condition

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 420 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* [vrf *vrf-name*]	Mandatory. By default, no DHCP address pool has been created by the system.

Note

- Address pools fall into two types: Network and Range. The two types of address pools can be configured respectively through the network and range commands.

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 421 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* [vrf *vrf-name*]	-
Configure an IP address range for an address pool of the Network type.	network *ip-address* [*network-mask* | *mask-len*]	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* | *mask-len*]	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.
- Modify the network type of address pool to the range type (or change the range type of address pool to the network type). If the new address range intersects with the old address range, the command line will prompt the user whether to perform the operation. If yes, delete all address configurations (static binding, vendor sub pool) in the and dynamic lease; if the actual effective range of the new address contains the actual effective range of the old address, the address pool will reserve all the address configurations in the address pool (static binding, vendor sub-pool), but will delete the configured ip range and dynamic lease of the vendor sub-pool.

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 422 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* [vrf *vrf-name*]	-
Configure a DNS server address.	dns-server { *ip-address*&<1-8> | autoconfig }	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 423 Configuring the Default Route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configure the default route.	default-router *ip-address*&<1-8>	Mandatory. By default, no default route is configured.

Configure domain-name

On the DHCP server, domain name information can be configured separately for each DHCP address pool. When assigning IP addresses to DHCP clients, the DHCP server also sends domain name information to the clients.

When the DHCP client performs dynamic domain name resolution, add a valid domain name to the DNS server.

Table 424 Configure domain-name

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configure domain-name	domain-name *string*	Mandatory By default, do not configure the domain name information.

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 425 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* [vrf *vrf-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.

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 426 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* **[vrf** *vrf-name* **]**	-
Bind an IP address and a MAC address.	**bind** { *ip-address mac-address* | **automatic**}	Mandatory. By default, no IP address and MAC address binding is configured.

Configure bootfile Field

Configure the boot filename field of the DHCP server protocol header to carry information.

Table 427 Configure the custom option of the user

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configure the boot filename field of the DHCP server protocol header to carry information.	bootfile *string*	Mandatory By default, the boot filename field of the DHCP server protocol header does not carry information.

Configure the next-server Field

Configure the next server ip address field of the DHCP server protocol header to carry the IP address information.

Table 428 Configure the custom option of the user

Step	Command	Description

Enter the global configuration mode.	configure terminal	-
Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configure the next server ip address field of the DHCP server protocol header to carry the IP address information.	next-server *ip-address*	Mandatory By default, configure the IP address information carried by the next server ip address field of the DHCP server protocol header is the zero address.

Configure Custom Options

For some options, RFC does not give specifications; therefore, you can define these options according to the actual requirement.

Table 429 Configuring Custom Options

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configuring custom options.	option *option-code* { ascii *ascii-string* | hex *hex-string* | ip *ip-address*&<1-8> }	Mandatory. By default, custom options are not configured.

Configure the Address Pool of the DHCP Manufacturer

When the client requests the IP address, it may carry the option 60 option, indicating the manufacturer ID. The customer can specify different IP address sections for different manufacturers.

Table 430 Configure the DHCP manufacturer address pool

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

Enter the DHCP configuration mode.	ip dhcp pool *pool-name* [vrf *vrf-name*]	-
Configure the manufacturer address pool and enter the DHCP manufacturer address pool configuration mode	vendor-class-identifier *vendor_id*	By default, do not configure the manufacturer address pool.
Configure the manufacturer address pool range	ip range *low-ip-address high-ip-address*	By default, do not configure the range.
Configure the content of the option 43 returned for the specified manufacturer	option 43 { ascii *ascii-string* | hex *hex-string* | ip *ip-address*&<1-8> }	By default, do not configure.

5.3.2.2 Configure Other Parameters of a DHCP Server

Configuration Condition

None

Configure a DHCP Server

After configuring the interface to work in the DHCP server mode, when the interface receives the DHCP request packet sent by the DHCP client, the DHCP server will distribute the IP address and other network parameters for the client.

Table 431 Configure a DHCP server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the DHCP server function	ip dhcp server	Mandatory By default, do not configure the DHCP server function.

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 432 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*] [vrf *vrf-name*]	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 433 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 *milliseconds* }	Mandatory. By default, the number of ping packets is 1, and the timeout time is 500 ms.

Configure the DHCP Data Log Function

After enabling the data log function of the DHCP server, the distributed address

pool on the DHCP server is recorded to the data log.

Table 434 Configure the DHCP data log function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the data log function of the DHCP server	ip dhcp logging security-data	Mandatory By default, do not enable the data log function.

Configure Lease Update of DHCP Address Pool

Configure the lease update time of the DHCP server, and the lease information formed by the address pool on the DHCP server will be written to the file.

Table 435 Configure lease update time of DHCP address pool

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the lease update interval of the DHCP server	ip dhcp server database update {now| internal *seconds*	Mandatory By default, the lease is updated every 3600s.

Configure DHCP Server to Support Unicast Reply

When the interface receives the packet sent by the DHCP client, the DHCP server needs to reply the packet directly to the client. At this time, the DHCP server determines according to the flags of the DHCP protocol

If the flags require unicast reply to the client, the DHCP server will reply the client packet directly to the client by unicast packet.

Table 436 Configure the DHCP server to support unicast reply

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

Configure the DHCP server to support unicast reply	ip dhcp server enable-unicast	Mandatory By default, the DHCP server replies the client by the broadcast mode.

5.3.2.3 Configure the Functions of a DHCP Client

Configuration Condition

None

Configure a DHCP Client

A DHCP client interface obtains an IP address and other parameters through DHCP.

Table 437 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.

Configure the DHCP Route Distance

In IP routing table, each protocol has a management distance to control routing, that is, routing distance. Routing distance is used to make routing decisions for the same segment routes from different protocols. The route with small routing distance is prior.

Table 438 Configure the DHCP route distance

Step	Command	Description

Enter the global configuration mode.	configure terminal	-
Configure the DHCP route distance	ip dhcp route-distance *distance*	Mandatory By default, the DHCP route distance is 254.

Configure option 60 Function

The content of DHCP option 60 is manufacturer ID. When the DHCP client requests, it can carry the option 60. The server can customize the ip address distributing policy according to the option.

Table 439 Configure DHCP option 60 function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the option 60 function	ip dhcp vendor-class-identifier {disable | content *hex-string}*	By default, carry the option 60 option.

Configure DHCP Client Not to Request for Default Route Option

When the DHCP client request for the IP address, request for the default route by default. The user can specify the DHCP client not to request for the default route, but configure the route by self.

Table 440 Configure DHCP client not to request for the default route option

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure DHCP client not to request for the default route	ip dhcp router-option disable	Mandatory By default, the DHCP client

option		requests for the default route option.

5.3.2.4 Configure the Function of a DHCP Relay

Configuration Condition

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 441 Configuring a DHCP Relay

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the DHCP relay function.	ip dhcp relay	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 the DHCP client. If enabling the DHCP relay to support the Option 82 function, after the DHCP

relay receives the request packet sent by the DHCP client to the DHCP server and the request packet does not have the Option 82 option, add Option 82 in the request packet, and forward to the DHCP server. If enabling the DHCP relay to support Option 82, and the request packet has the Option 82 option, perform the next processing according to the action configured by the command **ip dhcp relay information strategy**, and then, forward the packet to the server. If the DHCP response packet received by the DHCP relay contains the Option 82 option, delete the Option 82 option, and then, forward the packet to the DHCP client.

Table 442 Configuring the Option82 Function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the DHCP relay to support the Option 82 option	ip dhcp relay information option	Mandatory By default, do not enable DHCP relay to support Option 82.
Configure the processing policy when the DHCP relay receives the request packet with Option 82 sent by the client	ip dhcp relay information strategy{drop | keep | replace}	Optional Use the replace action for the packet with Option 82.
Configure the Option82 function.	ip dhcp relay information option | remote-id { ascii *ascii-string* | hex *hex-string* }| circuit-id { ascii *ascii-string* | hex *hex-string* } }	Mandatory. By default, the Option82 function is not configured.

Configure Source Address of DHCP Relay

DHCP relays the DHCP client to the source address of the server packet. By default, use the address of the egress interface of the route to the DHCP server. In some special environment, the DHCP server cannot communicate with the address. Therefore, users can configure the source address of the DHCP relay packet to the

DHCP server and the giaddr field in the packet through the **ip dhcp relay source-address** command. Users also can configure the source address of the DHCP relay to be the interface address of the received DHCP client packet through the **ip dhcp relay source-address relay-address** command.

Table 443 Configure the source address of the DHCP relay packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the source address of the DHCP relay packet	ip dhcp relay source-address relay-address	Mandatory By default, the source address of the DHCP relay packet is the egress interface address of the route to the DHCP server.
Enter the interface configuration mode	interface *interface-name*	-
Configure the source address of the DHCP relay packet	ip dhcp relay source-address *ip-address*	Mandatory By default, the source address of the DHCP relay packet is the egress interface address of the route to the DHCP server.

Note

- The source address configured by the **ip dhcp relay source-address** *ip-address* command should be the interface address of the device. Meanwhile, the interface address should belong to the same vrf as the relay interface. Otherwise, the relay packet cannot be sent successfully.
- If the **ip dhcp relay source-address** *ip-address* command is configured in the interface mode, and the **ip dhcp relay source-address relay-address** command is configured in the global mode, the priority of the former is

higher than the latter. The DHCP relay will use the configured *ip-address* to fill in the source address of the packet sent by the DHCP relay to the DHCP server.

Configure the Address of the DHCP Server

When the interface receives the DHCP packet sent by the DHCP client, relay the packet to the configured DHCP server, which distributes the IP address.

Table 444 Configure the address of the DHCP server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the address of the DHCP server	ip dhcp relay server -address *ip-address*	Mandatory By default, do not configure the address of the DHCP server.

5.3.2.5 DHCP Monitoring and Maintaining

Table 445 DHCP Monitoring and Maintaining

Command	Description
clear ip dhcp pool *pool-name* { lease | conflict [*ip-address*] }	Clear the dynamic lease information or conflict address information in the address pool
clear ip dhcp server interface [*interface-name*] statistics	Clear the key information statistics when the DHCP server interacts packets with the client or relay
clear ip dhcp relay statistics	Clear the statistics information on the DHCP relay device
show ip dhcp server interface *interface-name* [statistics]	Display the associated address pool information in the specified interface or display the key information statistics when the DHCP server in

	the specified interface interacts packets with the client or relay
show ip dhcp pool *pool-name* { summary | ping_list | offer_list | excluded_list | conflict_list | lease | binding }	Display the summary information of the specified address pool or the address information of the ping check or the information about the address that has sent OFFER packet and is waiting for DHCP client to reply the REQUEST packet or display the exclude address information in the address pool or display the conflict address information in the address pool or display the dynamic lease information in the address pool or display the static binding information in the address pool.
show ip dhcp pool *pool-name* specific { ip-address *ip-address* | mac-address *mac-address* }	Display the specified ip address or mac address information in the address pool
show ip dhcp relay [interface *interface-name*]	Display the packet statistics information on the DHCP relay device

5.3.3 DHCP Typical Configuration Example

5. 3. 3. 1 Configure a DHCP Server to Statically Allocate IP Addresses

Network Requirements

- Device2 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 PC in MAC binding mode.

Network Topology

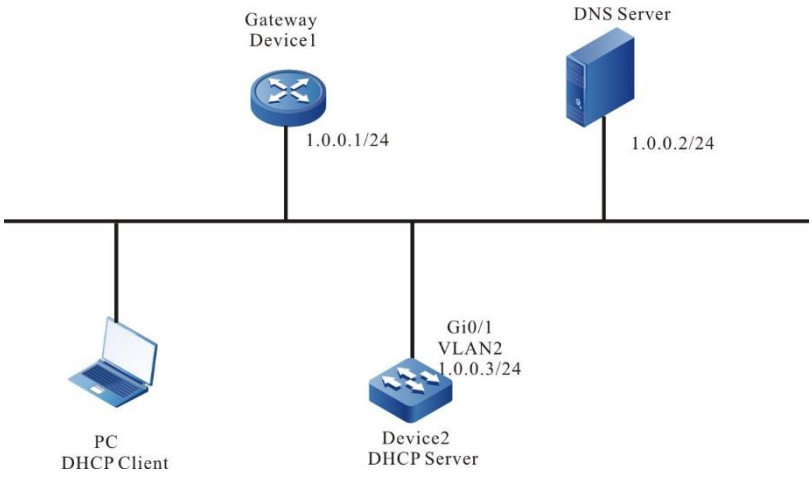


Figure 73 Configuring a DHCP Server to Statically Allocate IP Addresses

Configuration Steps

Step 1: Configure the IP address of the Device2 interface and works in the DHCP server mode.

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip address 1.0.0.3 255.255.255.0
Device2(config-if-vlan2)#ip dhcp server
Device2(config-if-vlan2)#exit
```

Step 2: Configure the static binding address pool and parameters.

#Configure the address pool mac-binding, and adopt the static mac binding mode to distribute IP address for the PC.

```
Device2(config)#ip dhcp pool mac-binding
Device2(dhcp-config)#range 1.0.0.4 1.0.0.254 255.255.255.0
Device2(dhcp-config)#bind 1.0.0.11 00e0.00c1.013d
Device2(dhcp-config)#default-router 1.0.0.1
Device2(dhcp-config)#dns-server 1.0.0.2
Device2(dhcp-config)#exit
```

Step 3: Check the result.

#On Device2, query the associated address pool of the interface via the **show ip dhcp server interface vlan2** command.

```
Device2(config)#exit
Device2#show ip dhcp server interface vlan2
```

```
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP      Pool name          Pool Range         Pool utilization
-----------   ------------------  ------------------  ----------------
 1.0.0.3/24       mac-binding      1.0.0.4 - 1.0.0.254        0.00%
```

#On Device2, query the binding IP address distributed for the PC via the **show ip dhcp pool mac-binding binding** command.

```
Device2#show ip dhcp pool mac-binding binding
IP Address     MAC Address       Vendor Id    Type     Time Left(s)
------------ ----------------- ------------ -------- -------------
1.0.0.11       00e0.00c1.013d       Global    Binding       NA
```

#On Device2, query the address distributed for the PC via the **show ip dhcp pool mac-binding lease** command.

```
Device#show ip dhcp pool danymic-pool2 lease
IP Address       MAC Address       Vendor Id       Type    Time Left(s)
------------ ------------------ ------------------- -------- ---------
----
1.0.0.11       00e0.00c1.013d       Global        Lease    107980
```

On the PC, check whether the got IP address, gateway IP address, and DNS server address are correct.

5.3.3.2 Configure a DHCP Server to Dynamically Allocate IP Addresses

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 2.0.0.0.0/24 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. 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.

- The first 10 IP addresses in network segments 1.0.0.0/24 are reserved and cannot be allocated.

Network Topology

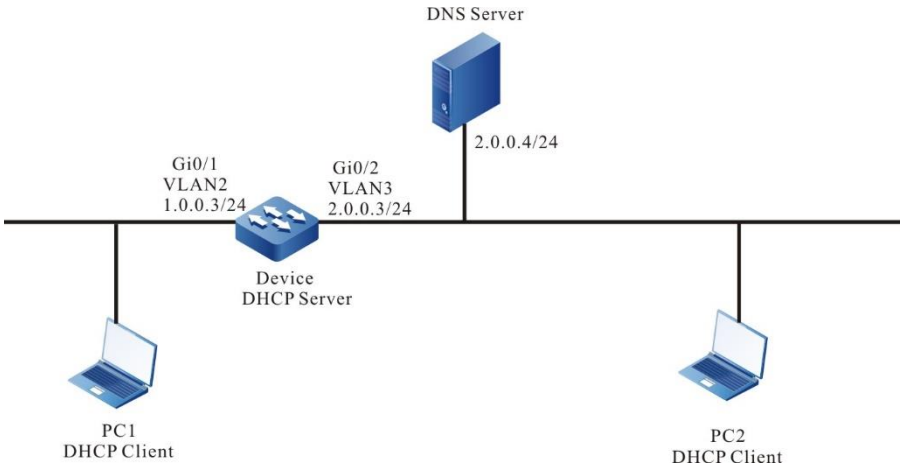


Figure 74 Networking for Configuring DHCP to Dynamically Allocate IP Addresses

Configuration Steps

Step 1: Configure the IP address of the interface of the device, and make the interface work in the DHCP server mode.

```
Device(config)#interface vlan2
Device(config-if- vlan2)#ip address 1.0.0.3 255.255.255.0
Device(config-if- vlan2)#ip dhcp server
Device(config-if- vlan2)#exit
Device(config)#interface vlan3
Device(config-if- vlan3)#ip address 2.0.0.3 255.255.255.0
Device(config-if- vlan3)#ip dhcp server
Device(config-if- vlan3)#exit
```

Step 2: On the DHCP server Device, configure two dynamic address pools and their parameters.

#Configure the first 10 IP addresses in the two address pools as the

reserved addresses.

```
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 the address pool named dynamic-pool1 and the parameters (address range, gateway, dns address, and address lease).

```
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)#lease 1 0 0
Device(dhcp-config)#exit
```

#Configure the address pool named dynamic-pool2 and the parameters (address range, gateway, dns address, and address lease).

```
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)#lease 3 0 0
Device(dhcp-config)#exit
```

Step 3: Check the result.

#Query the information of the associated address pool of the server on Device.

```
Device(config)#exit
Device#show ip dhcp server interface vlan2
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP      Pool name          Pool Range        Pool utilization
-----------  ------------------  -------------------  -----------
-----
1.0.0.3/24       dynamic-pool1     1.0.0.0 – 1.0.0.255       0.00%
Device#show ip dhcp server interface vlan3
DHCP server status information:
DHCP server is enabled on interface: vlan3
Vrf : global
DHCP server pool information:
```

```
Available directly-connected pool:
Interface IP      Pool name         Pool Range        Pool utilization
------------      ------------------    --------------------    ------------
1.0.0.3/24      dynamic-pool2       2.0.0.0 – 2.0.0.255       0.00%
```

#Query the IP address information distributed for the client on Device.

```
Device#show ip dhcp pool danymic-pool1 lease
IP Address       MAC Address       Vendor Id       Type    Time Left(s)
------------   ---------------  ----------------   --------  ------------
1.0.0.11         0101.7a6a.0268       Global       Lease     86390
Device#show ip dhcp pool danymic-pool2 lease
IP Address       MAC Address       Vendor Id       Type    Time Left(s)
------------   ------------------   --------------   --------  ------------
2.0.0.11         0101.7a6a.0269       Global       Lease     259194
```

#Query the distribution statistics information of the configured IP address pool on Device.

```
Device#show ip dhcp pool dynamic-pool1 summary
Pool: dynamic-pool1
Pool Configuration  : 1.0.0.0  255.255.255.0
Pool Range          : 1.0.0.0  1.0.0.255
Pool Utilization    : 0.39%
VRF                 : global
DNS Server          : 2.0.0.4
Default Router      : 1.0.0.3
Lease Time          : 1 Days 0 Hours 0 Minutes
Free Addresses      : 243
Static Bind         : 0
Lease Count         : 1
PingList            : 0
OfferList           : 0
ConflictList        : 0
ExcludeList         : 12
```

Device#show ip dhcp pool dynamic-pool2 summary

```
Pool: dynamic-pool2
Pool Configuration  : 2.0.0.0  255.255.255.0
Pool Range          : 2.0.0.0  2.0.0.255
Pool Utilization    : 0.39%
VRF                 : global
```

```
DNS Server        : 2.0.0.4
Default Router    : 2.0.0.3
Lease Time        : 3 Days 0 Hours 0 Minutes
Free Addresses    : 243
Static Bind       : 0
Lease Count       : 1
PingList          : 0
OfferList         : 0
ConflictList      : 0
ExcludeList       : 12
```

On the DHCP client, query whether the IP addresses have been obtained properly.

Caution

- The IP address in the address pool should belong to the segment range of the interface providing the service.

5.3.3.3 Configure a DHCP Relay

Network Requirements

- Device1 is the DHCP server, and the interface of Device2 enables the DHCP relay function.
- The DHCP server provides the service for the client of the segment 1.0.0.0/24, and the first ten IP addresses are reserved.
- The DHCP client gets the IP address via DHCP relay.

Network Topology

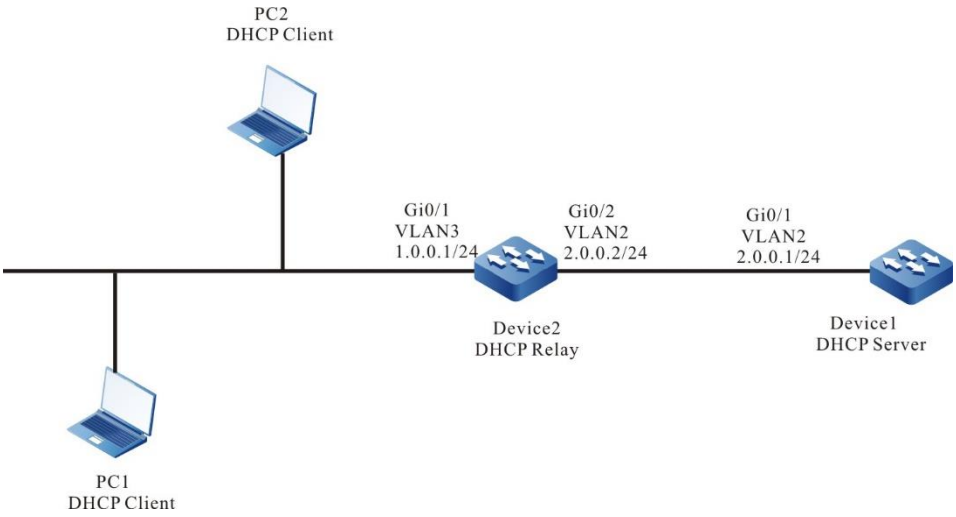


Figure 75 Networking for Configuring a DHCP Relay

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN. Configure the IP address of the interface (omitted).

Step 2: Configure the IP address pool of Device1 and the reserved IP address, and work in the DHCP server mode.

#Configure the DHCP server.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
```

#Configure the IP addresses of 1.0.0.1 to 1.0.0.10 not to be distributed.

```
Device1#configure terminal
Device1(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
```

#Configure the IP address pool of Device1 dynamic-pool.

```
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 the static route to the segment 1.0.0.0/24.

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

Step 3: On the vlan3 interface of Device2, configure the address of the DHCP server as 2.0.0.1, and make the interface work in the relay mode.

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-addres 2.0.0.1
Device2(config-if-vlan3)#exit
```

Step 4: Check the result.

#Query the information of the IP address distributed on Device1.

```
Device1#show ip dhcp pool dynamic-pool lease
IP Address      MAC Address      Vendor Id      Type   Time Left(s)
------------   --------------   ---------------  --------   -----------
1.0.0.11       0101.7a6a.0268       Global       Lease      86387
```

Use the **show ip dhcp pool dynamic-pool lease** command to query the IP address that has been allocated to the client. The result shows that the client has obtained the IP address 1.0.0.12.

5.3.3.4 Configure the DHCP Relay to Support Option82

Network Requirements

- On the DHCP relay device, Option82 is enabled.
- For Option82 sub-option Remote ID, specify the content as 0102030405.
- The DHCP relay Device2 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

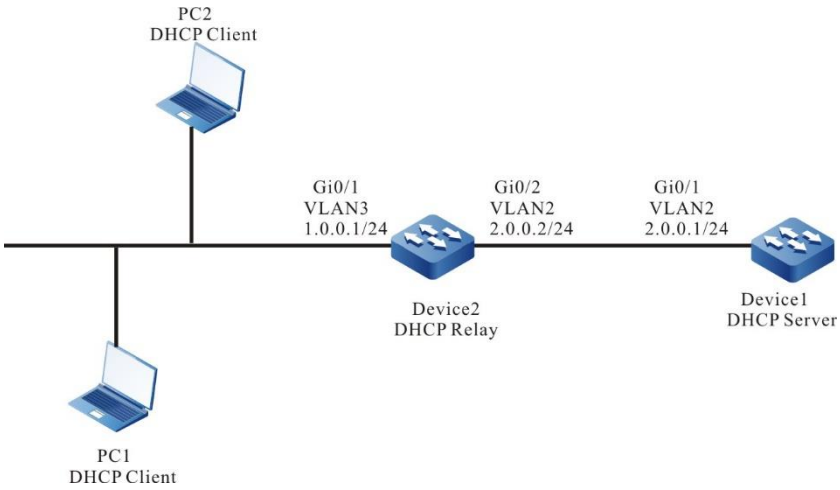


Figure 76 Networking for Configuring the DHCP Relay to Support Option82

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN. Configure the IP address of the interface (omitted).

Step 2: Configure the DHCP server.

```
Device1# configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
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)#exit
```

#Configure the static route to the segment 1.0.0.0/24.

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

Step 3: Configure the DHCP relay device Device2 and Option82 parameters.

#Configure the IP address of the DHCP relay server as 2.0.0.1.

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-address 2.0.0.1
```

#Enable Option82, and configure the sub option remote-ID as 0102030405.

```
Device2(config)#ip dhcp relay information option
Device2(config)#ip dhcp relay information remote-id hex 0102030405
```

Step 4: Check the result.

Query the information of the IP address distributed for the client on Device1.

```
Device1#show ip dhcp pool danymic-pool1 lease
IP Address      MAC Address       Vendor Id       Type   Time Left(s)
--------------- ----------------- ------------------- -------- -------------
1.0.0.2         0101.7a6a.0268    Global          Lease  107992
```

On the DHCP client, query one IP address of the segment 1.0.0.0/24 got by the network card.

On the DHCP server, capture the packet, and you can verify that the remote-id of option82 in the discover packet received by the server is 0102030405.

Note

- After Option82 is enabled, its sub-option Circuit ID is filled with the receiving interface index and the system ID of the relay device.

5.4 DNS

5.4.1 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.

5.4.2 DNS Function Configuration

Table 446 DNS Function List

Configuration Tasks	
Configure the DNS cache specification	Configure the maximum specification of the static cache
	Configure the maximum specification of the dynamic cache
Configure the DNS client function.	Configure static domain name resolution.
	Configure dynamic domain name resolution.
Configure the DNS detection function	Configure the domain name list
	Detect the domain name resolution

5.4.2.1 Configure DNS Cache Specification

Configuration Condition

None

5.4.2.1.1 Configure DNS Specification

When modifying the maximum specification supported by DNS, if the current specification is M, the current quantity is n, and the configured specification is N. There are the following scenarios:

1. Static specification: If N > M or n < N < M, the configuration takes effect immediately; if N<n, the system prompts that the configuration fails.
2. Dynamic specification: If N > M or n < N < M, the configuration takes effect immediately; if N<n, the configuration takes effect, and wait for the dynamic quantity to age.

Table 447 Configure the authentication method list of the privileged mode

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the maximum specification supported by static dns	dns static max-count *number*	Optional By default, the static cache supports 64 at most.
Configure the maximum specification supported by dynamic dns cache	dns dynamic max-count *number*	Optional By default, the dynamic cache supports 10K at most.

5.4.2.2 Configure the DNS Client Function

Configuration Condition

None

Configure Static Domain Name Resolution

In configuring static domain name resolution, you can configure a domain names to map the IPv4 address and IPv6 address.

Table 448 Configuring Static Domain Name Resolution

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the corresponding IPv4 address of the static domain name	ip host [vrf vrf-name] domain-name ip-address	Mandatory By default, do not configure the corresponding IPv4 address of the domain name.

Step	Command	Description
Configure the corresponding IPv6 address of the static domain name	ipv6 host [vrf vrf-name] domain-name ipv6-address	Mandatory By default, do not configure the corresponding IPv6 address of the domain name.

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 449 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.

5.4.2.3 Configure DNS Detection Function

Configuration Condition

None

Configure Domain Name List

Configure the domain name list, and you can add some common domain names to the domain name list for saving. When it is necessary to use, directly specify the name of the domain name list.

Table 450 Configure the domain name list

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one domain name list and enter the domain name list configuration mode	dns domain-list *list-name*	Mandatory By default, do not configure the domain name list.
Configure the domain name	domain *domain-name*	Mandatory By default, do not configure the domain name in the domain name list.

Detect Domain Name Resolution

Detect the domain name resolution, and you can detect whether the DNS server can correctly resolve the specified domain name.

Table 451 Detect the domain name resolution

Step	Command	Description
Detect the domain name resolution	dns query [vrf *vrf-name*] *ip-address* [name *domain-name* | name-list *list-name*] [timeout *time*]	Mandatory By default, do not detect the domain name resolution.

5.4.2.4 DNS Monitoring and Maintaining

Table 452 DNS Monitoring and Maintaining

Command	Description
debug dns {all | config | event | mpos | packet | timer}	Enable the DNS debugging information

Command	Description
show dns domain-list [*list-name*]	Display the domain name list
show hosts	Display the entries of the domain name resolution list
show name-server [vrf *vrf-name*]	Display the DNS server information

5.4.3 DNS Typical Configuration Example

5.4.3.1 Configure Static Domain Name Resolution

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

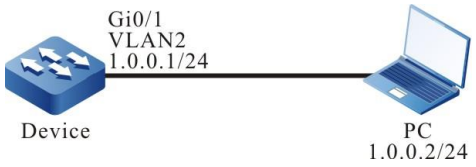


Figure 77 Networking for Configure Static Domain Name Resolution

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
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.

5.4.3.2 Configure Dynamic Domain Name Resolution

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

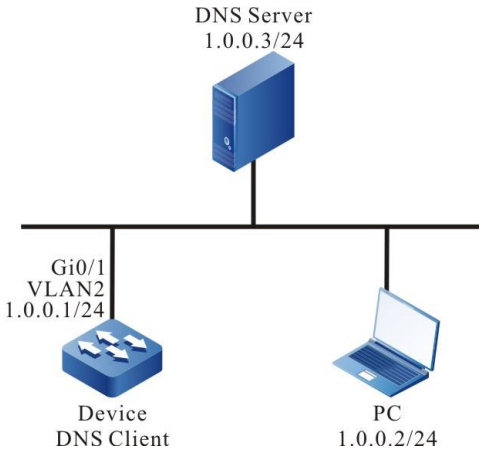


Figure 78 Networking for Configure Dynamic Domain Name Resolution

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
Device(config)#exit
```

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
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.
```

5.5 IPv6 Basis

5.5.1 Overview

IPv6 (Internet Protocol Version 6) is the second generation standard protocol of the network layer protocol, also known as IPng (IP Next Generation). It is a set of specifications designed by IETF (Internet Engineering Task Force) and an upgraded version of IPv4.

L3 interface ND proxy

L3 interface ND proxy is used to realize interworking of different network segments connected through two interfaces. Generally, the device will not respond to the NS request whose target is not the network segment corresponding to the packet receiving interface, so different network segments cannot directly communicate with each other. When the ND proxy function is enabled on the L3 interface, if the device receives NS belonging to other interface network segments from the interface, it can also respond to NA. Thus, the hosts belonging to different network segments can also establish neighbor entries and communicate normally. Its typical application scenario is the networking of large and small network segments.

5.5.2 IPv6 Basic Function Configuration

Table 453 IPv6 basic function configuration list

Configuration Tasks	
Configure the IPv6 address	Configure the interface IPv6 address
Configure IPv6 basic functions	Enable the IPv6 unicast forwarding function
	Enable the interface IPv6 function
	Configure the IPv6 packet hop limit
	Configure the IPv6 MTU of the interface
Configure the IPv6 neighbor discovery protocol	Configure the IPv6 static neighbor
	Configure the aging time of the IPv6 neighbor entry in the STALE state
	Configure the interval of re-transmitting the NS packet
	Configure the times of sending the NS packet when

Configuration Tasks	
	IPv6 repeats the address detection
	Configure the related parameters of the RA packet
	Enable the function of the interface sending the re-direct packet
Enable the ND quick response function	Enable the ND quick response function
Configure the L3 interface ND proxy function	Configure the L3 interface ND proxy function
Configure the ICMPv6 function	Configure the rate of sending the ICMPv6 error packet
	Enable the function of sending the ICMPv6 packet with unreachable destination
Configure the IPv6 TCP anti-attack function	Enable the TCP syncache function
	Enable the TCP syncookies function

5.5.2.1 Configure Interface IPv6 Address

The most striking difference between IPv6 and IPv4 is that the length of the IP address increases from 32 bits to 128 bits. The IPv6 address is represented as a series of 16-bit hex numbers separated by colon (:). Each IPv6 address is divided into eight groups, each group of 16 bits represented by four hexadecimal digits, and the groups are separated by colons, such as 2000:0000:240F:0000:0000:0CB0:123A:15AB.

In order to simplify the representation of the IPv6 address, process the “0” in the IPV6 address as follows:

The preamble “0” in each group can be omitted, that is, the above address can be represented as 2000:0:240F:0:0:CB0:123A:15AB.

If the address contains two or more consecutive groups of zero, it can be replaced by a double colon "::" that is, the above address can be represented as 2000:0:240F:: CB0:123A:15AB.

The double colon "::" can only be used once in an IPv6 address. Otherwise, the number of zeros represented by "::" cannot be determined when the device converts "::" to zero to recover 128-bit addresses.

The IPv6 address consists of two parts: address prefix and interface identifier. The address prefix is equivalent to the network number field in the IPv4 address and the interface identifier is equivalent to the host number field in the IPv4 address.

The IPv6 address prefix is expressed as: IPv6 address/prefix length. The IPv6 address is any of the forms listed above, and the prefix length is a decimal number that indicates how many bits in front of the IPv6 address is the address prefix.

There are three kinds of IPv6 addresses, that is, unicast address, multicast address, and anycast address:

Unicast address: used to uniquely identify an interface, similar to IPv4 unicast address. The packets sent to one unicast address will be sent to the interface identified by this address.

Multicast address: used to identify a set of interfaces, similar to IPv4 multicast address. The packets sent to one multicast address are sent to all the interfaces identified by this address.

Anycast Address: used to identify a group of interfaces and the packet whose destination is an anycast address is sent only to one interface in the group. According to the routing protocol, the interface of receiving the packet is the closest interface from source.

The IPv6 address type is specified by the first few bits of the address, called the format prefix. The corresponding relationship between the main address type and the format prefix is shown in Table.

Table 454 The corresponding relationship between the IPv6 address type and the format prefix

Address Type		Format Prefix (Binary)	Prefix ID
Unicast address	Un-specified address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128

Address Type		Format Prefix (Binary)	Prefix ID
	The local address of the link	1111111010	FE80::/10
	The local address of the site	1111111011	FEC0::/10
	Global unicast address	Other forms	-
Multicast address		11111111	FF00::/8
Anycast address		Distributed from the unicast address space, use the format of the unicast address	

IPv6 unicast addresses can be of various types, including global unicast addresses, link local addresses, and site local addresses.

The global unicast address is equivalent to the IPv4 public network address, which is provided to the Internet service provider. This type of addresses allows the aggregation of routing prefixes, thus limiting the number of global routing entries.

Link local addresses are used for the communication between the local nodes on the link in the neighborhood discovery protocol and stateless automatic configuration. The packet using the link local address as the source or destination address is not forwarded to other links.

The local address of the site is similar to the private address in IPv4. The packet using the local address of the site as the source or destination address is not forwarded to other sites outside the site.

Loopback address: Unicast address 0:0:0:0:0:0:0:0:1 (simplified as: 1) is called a loopback address and cannot be assigned to any physical interface. Its function is the same as the loopback address in IPv4, that is, the node sends IPv6 packets to itself.

Un-specified address: The address “::” is called an unspecified address and

cannot be assigned to any node. Before a node obtains a valid IPv6 address, it can be entered in the source address field of the IPv6 packet sent, but not as the destination address of the IPv6 packet.

The special multicast addresses reserved by IPv6 are shown in table.

Table 455 The special multicast address list of IPv6

Address	Usage
FF01::1	The multicast address of all nodes in the local scope of the node
FF02::1	The multicast address of all nodes in the local scope of the link
FF01::2	The multicast address of all routers in the local scope of the node
FF02::2	The multicast address of all routers in the local scope of the link
FF05::2	The multicast address of all routers in the local scope of the site

Configuration Condition

None

Configure the IPv6 Address of the Interface

Table 456 Configure the IPv6 address of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IPv6 address of the interface	ipv6 address { *linklocal-address* link-local | *prefix-address* [anycast | eui-64] | autoconfig }	Mandatory By default, the interface is not configured with the IPv6 address.

Note

- One interface can be configured with multiple IPv6 addresses.

- After one interface is configured with the IPv6 address, automatically enable the IPv6 function.

5.5.2.2 Configure IPv6 Basic Functions

Configuration Condition

None

Enable IPv6 Unicast Forwarding Function

By default, the IPv6 unicast forwarding function is enabled. In some special cases, the user can disable the IPv6 unicast forwarding function. After disabling the function, do not forward the IPv6 packet.

Table 457 Enable IPv6 unicast forwarding function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable IPv6 unicast forwarding function	ipv6 unicast-routing	Mandatory By default, the IPv6 unicast forwarding function is enabled.

Enable IPv6 Function of the Interface

Before performing the IPv6 configuration on one interface, first enable the IPv6 function. Otherwise, some configuration will not take effect.

Table 458 Enable the IPv6 function of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the IPv6 function of the interface	ipv6 enable	Mandatory By default, the IPv6 function of

		the interface is disabled.

Configure the Hop Limit of the IPv6 Packet

The IPv6 header contains the Hop Limit field, whose function is the same as the TTL field in the IPv4 header, representing the times the packet can be forwarded by the router over the network.

With the command, you can configure the hop limit in the IPv6 packet header generated by the device.

Table 459 Configure the hop limit of the IPv6 packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the hop limit of the IPv6 packet	ipv6 hop-limit *value*	Mandatory By default, the hop limit of the IPv6 packet sent by the device is 64.

Configure the IPv6 MTU of the Interface

Table 460 Configure the IPv6 MTU of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IPv6 MTU of the interface	ipv6 mtu *value*	Mandatory By default, do not configure the IPv6 MTU of the interface

.

5.5.2.3 Configure IPv6 Neighbor Discovery Protocol

IPv6 Neighbor Discovery protocol includes the following functions: address resolution, neighbor unreachable detection, duplicate address detection, router discovery / prefix discovery, address auto configuration and redirection.

The ICMPv6 packet type used by the ND protocol and its functions are shown in

the following table.

Table 461 The ICMPv6 packet type used by the ND protocol and its functions

ICMPv6 Packet Type	Type No.	Function
Router request packet (RS: Router Solicitation)	133	After a node starts, it sends a request to the router via the RS packet, requesting the prefix and other configuration information, used for auto configuration of the node
Router advertisement packet (RA: Router Advertisement)	134	Respond for the RS packet Without suppressing the sending of RA packets, the router periodically sends RA packets, including prefix information options and some flag bits.
Neighbor request packet (NS: Neighbor Solicitation)	135	Get the link-layer address of the neighbor Verify whether the neighbor is reachable Perform the repeated address detection
Neighbor advertisement packet (NA: Neighbor Advertisement)	136	Respond for the NS packet The node sends the NA packet automatically when the link layer changes, advertising the change information of the node to the neighbor node.
Re-direction packet (Redirect)	137	When meeting a certain condition, the default gateway sends a redirect packet to the source host, making the host re-select the correct next hop address for subsequent packet transmission.

- Address resolution
- Get the link-layer address of the neighbor node on one link, which is realized by the NS packet and NA packet
- Neighbor unreachable detection
- After getting the link-layer address of the neighbor node, verify whether the neighbor node is reachable via the NS packet and NA packet.
- The node sends the NS packet, whose the destination address is the IPv6 address of the neighbor node

- If receiving the confirm packet of the neighbor node, it is regarded that the neighbor is reachable. Otherwise, it is regarded that the neighbor is not reachable.
-
- Duplicate address detection
- After the node gets one IPv6 address, it is necessary to use the duplicate address detection function to confirm whether the address is used by other nodes.
- Router discovery/prefix discovery and address auto configuration
- Router discovery/prefix discovery indicates the node gets the neighbor router and its network prefix from the received RA packet, as well as other configuration parameters.
- Address stateless auto configuration indicates that the node automatically configures the IPv6 address according to the information obtained by router discovery / prefix discovery.
- Router discovery/prefix discovery is achieved through RS packets and RA packets.
- Re-direction
- When the host starts, there may be only one default route to the default gateway in its routing table. When meeting certain conditions, the default gateway sends ICMPv6 redirect packets to the source host, informing the host to choose a better next hop for sending the subsequent packets.

Configuration Condition

None

Configure IPv6 Static Neighbor

Resolving the IPv6 address of the neighbor node into the link layer address can be realized by the address resolution function of the IPv6 ND protocol, or by configuring the static neighbor manually.

The IPv6 neighbor is uniquely identified by the IPv6 address of the neighbor node and the L3 interface connected to the neighbor node.

Table 462 Configure the IPv6 static neighbor

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the IPv6 static neighbor	ipv6 neighbor *ipv6-address interface-name mac-address*	Mandatory By default, do not configure the IPv6 static neighbor.

Configure the Age Time of the IPv6 Neighbor Entry in the STALE State

IPv6 neighbor entries have five reachability states: INCOMPLETE, REACHABLE, STALE, DELAY and PROBE. The STALE state indicates not knowing whether the neighbor is reachable or not. The neighbor entry in STALE state has an aging time, and the neighbor entries in STALE state reaching the aging time will migrate to the DELAY state.

Table 463 Configure the age time of the IPv6 neighbor entry in the STALE state

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the age time of the IPv6 neighbor entry in the STALE state	ipv6 neighbor stale-aging *aging-time*	Optional By default, the age time of the IPv6 neighbor entry in the STALE state is 7200s.

Configure the Re-transmission Interval of the NS Packet

When the device sends an NS packet, and if it does not receive a response within a specified time interval, it will resend the NS packet. The interval for re-sending NS

packet can be configured by the following command.

Table 464 Configure the interval of re-sending the NS packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the re-transmission interval of the NS packet	ipv6 nd ns-interval *value*	Mandatory By default, the interval of sending the NS packet is 1000ms.

Configure the Times of the IPv6 Duplicate Address Detection Sending the NS Packet

After the interface is configured with the IPv6 address, the NS packet is sent for duplicate address detection. If no response is received within a certain period of time, the NS packet is continued to be sent. When the number of NS packets sent reaches the set value, no response is received, the address is considered available.

Table 465 Configure the times of the IPv6 duplicate address detection sending the NS packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the times of the IPv6 duplicate address detection sending the NS packet	ipv6 nd dad attempts *value*	Mandatory By default, the times of the IPv6 duplicate address detection sending the NS packet is 1.

Configure the Related Parameters of the RA Packet

Users can configure whether the interface sends the RA packet and the interval of sending the RA packet according to the actual situation, and can configure the

parameters of the RA packet to inform the host. When the host receives the RA message, it can use these parameters to do the corresponding operation.

Table 466 The parameters and descriptions in the RA packet

Parameter	Description
Hop Limit	When sending the IPv6 packet, the host will fill the Hop Limit field in the IPv6 header using this parameter value. At the same time, the parameter value is also used as the Hop Limit field value in the device reply packet.
MTU	The MTU of the released link, which can be used to ensure that all nodes on one link adopt the same MTU value
Router Lifetime	Used to set the time of the router that sends the RA packet serving as the default router of the host. The host can determine whether to take the router sending the RA packet as the default router based on the router lifetime parameter value of the received RA packet.
The time of the neighbor keeping the reachable state (Reachable Time)	When the neighbor reachability detection confirms that the neighbor is reachable, the device assumes that the neighbor is reachable within the set reachable time; if a packet needs to be sent to the neighbor after the set time, reconfirm that the neighbor is reachable.

Table 467 Configure the related parameters of the RA packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the prefix option information in the RA packet	ipv6 nd prefix { *ipv6-prefix* | default } [*valid-lifetime* | infinite | no-advertise | no-autoconfig | off-link] [*prefered-lifetime* | infinite]	Mandatory By default, do not configure the prefix option information.
Configure the value of the Hop Limit field in the RA packet	ipv6 nd ra hop-limit	Optional By default, do not configure the

sent by the interface to be got from the global configuration		value of the Hop Limit field in the RA packet sent by the interface to be got from the global configuration, and the value of the Hop Limit field is 0.
Configure the maximum interval and minimum interval of sending the RA packet	ipv6 nd ra interval *max-value* [*min-value*]	Optional By default, the maximum interval of sending the RA packet is 600s, and the minimum interval is 198s.
Configure the RA packet to carry the MTU option	ipv6 nd ra mtu	Optional By default, the RA packet does not carry the MTU option.
Configure the lifetime of the router in the RA packet	ipv6 nd ra-lifetime *value*	Optional By default, the lifetime of the router in the RA packet is 1800s.
Prohibit the interface from sending the RA packet periodically	ipv6 nd suppress-ra period	Optional By default, the interface does not send the RA packet periodically.
Prohibit the interface from replying the RS packet	ipv6 nd suppress-ra response	Optional By default, the interface does not reply the RA packet when receiving the RS packet.

Enable the Interface to Send the Re-Direct Packet

After receiving the IPv6 packet that needs to be forwarded, the device finds that the receiving interface of the packet is the same as the sending interface by selecting the route. At this time, the device forwards the packet and sends back the redirect packet to the source, informing the source to re-select the correct next hop for sending the subsequent packets. By default, a device can send a redirect packet, but in some

specific cases, the user can prevent the device from sending a redirect packet.

Table 468 Enable the function of the interface sending the re-direct packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the function of the interface sending the re-direction packet	ipv6 redirects	Optional By default, the function of the interface sending the re-direction packet is enabled.

5.5.2.4 Enable ND Fast Response Function

Configuration Condition

None

Enable ND Fast Response Function

Table 469 Enable ND fast response function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable ND fast response function	nd fast-response	Mandatory By default, the global ND fast response function is enabled.

5.5.2.5 Configure L3 Interface ND Proxy

Configuration Condition

None

Configure L3 Interface ND Proxy

Table 470 Configure L3 interface ND proxy

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L3 interface configuration mode	interface *interface-name*	Mandatory After entering the L3 interface configuration mode, the subsequent configuration takes effect only on the current interface.
Enter the global configuration mode	configure terminal	-
Configure the ND proxy function of the L3 interface	nd proxy enable	Mandatory By default, the interface does not enable the proxy function.

5.5.2.6 Configure ICMPv6 Function

In IPv6 protocol stack, Internet Control Message Protocol is mainly used to provide network detection services, and provide error reports to inform the corresponding devices when the network layer or transport layer protocol is abnormal, so as to control and manage the network.

Configuration Condition

None

Configure the Rate of Sending the ICMPv6 Error Packet

If there are too many ICMPv6 error packets sent in the network, it may lead to network congestion. To avoid this, users can configure the maximum number of ICMPv6 error packets sent within a specified time.

Table 471 Configure the rate of sending the ICMPv6 error packets

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Configure the rate of sending the ICMPv6 error packets	ipv6 icmp error-interval *interval* [*buckets*]	Optional By default, the period of sending the ICMPv6 error packets is 100ms, and the maximum number of the ICMPv6 error packets sent in the period is 10.

Enable the Function of Sending the ICMPv6 Packet with Unreachable Destination

The function of sending the ICMPv6 packet with the unreachable destination indicates that after receiving one IPv6 packet and if its destination is reachable, the device discards the packet and sends the ICMPv6 unreachable error packet to the source.

The device will send ICMPv6 unreachable error packet when meeting the following conditions:

- When forwarding packets, and if failed to find the route, the device sends the ICMPv6 error packet "No route to the destination address" to the source.
- When a device forwards a packet, and if it is unable to send it due to a management policy (such as firewall, ACL), it sends an ICMPv6 error packet "the communication with destination address is prohibited by management policy" to the source.
- If the destination IPv6 address of the packet exceeds the range of the source IPv6 address (for example, the source IPv6 address of the packet is the link local address, and the destination IPv6 address of the packet is the global unicast address) when forwarding a packet, and as a result, the packet cannot reach the destination, the device will send the ICMPv6 error packet "out of the source address range" to the source.
- If the device fails to resolve the link layer address of the destination IPv6

address when forwarding the packet, it sends the "address unreachable" ICMPv6 error packet to the source.

- When a device receives an IPv6 packet whose destination address is the local and transport layer protocol is UDP, and if the destination port number of the packet does not match the process in use, it sends a "port unreachable" ICMPv6 error packet to the source.

Because the information transmitted to the user process by ICMPv6 destination unreachable error packet is unreachable, if there is a malicious attack, it may affect the normal use of the terminal users. To avoid these phenomena, the user can disable the function of sending the ICMPv6 destination unreachable error packet.

Table 472 Enable the function of sending the ICMPv6 packet with the unreachable destination

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the function of sending the ICMPv6 packet with the unreachable destination	ipv6 unreachables	Optional By default, the function of sending the ICMPv6 packet with the unreachable destination is enabled.

5.5.2.7 Configure the IPv6 TCP Anti-Attack Function

If the IPv6 TCP server receives a large number of SYN packets, but the peer does not reply the SYN+ACK response to the server, this will lead to a large amount of memory consumption on the server, occupying the semi-connected queue of the server, and as a result, the IPv6 TCP server cannot serve the normal request. This attack can be avoided by configuring the IPv6 TCP anti-attack function.

Configuration Condition

None

Enable IPv6 TCP syncache Function

Instead of rushing to allocate TCB when receiving SYN packets, the function first

replies a SYN + ACK packet and stores this semi-open connection information in a dedicated cache until the correct ACK packet is received, and then reallocates the TCB.

Table 473 Enable IPv6 TCP syncache function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the IPv6 TCP syncache function	ipv6 tcp syncache	Mandatory By default, the IPv6 TCP syncache function is disabled.

Enable IPv6 TCP syncookies Function

This function does not use any storage resources at all. It uses a special algorithm to generate Sequence Number. This algorithm takes into account the IPv6 address and port of the peer party, the IPv6 address and port fixed information of one's own party, and some fixed information of one's own party that the peer party cannot know, such as MSS and time. After receiving the ACK packet of the peer party, recalculate it to see whether it is the same as the Sequence Number-1 in the response packet of the peer party, so as to decide whether to allocate TCB resources.

Table 474 Enable the IPv6 TCP syncookies function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the IPv6 TCP syncookies function	ipv6 tcp syncookies	Mandatory By default, the IPv6 TCP syncookies function is disabled.

5.5.2.8 IPv6 Basic Monitoring and Maintaining

Table 475 IPv6 basic monitoring and maintaining

Command	Description
clear nd fast-response statistics	Clear the ND fast response statistics
clear ipv6 icmp6stat	Clear the ICMPv6 statics information
clear ipv6 interface statistics	Clear the IPv6 packet statistics information of the interface
clear ipv6 mtu	Clear the MTU information of the IPv6 path

Command	Description
clear ipv6 neighbors	Clear the IPv6 dynamic neighbor entry
clear ipv6 statistics	Clear the IPv6 basic statistics information
clear ipv6 tcp syncache statistics	Clear the syncache statistics information of the IPv6 TCP protocol
clear ipv6 tcp6stat	Clear the IPv6 TCP statistics information
clear ipv6 udp6stat	Clear the IPv6 UDP statistics information
show nd fast-response statistics	Display the ND fast response statistics
show ipv6 hop-limit	Show the IPv6 global Hop Limit value
show ipv6 frag-queue	Show the cached IPv6 fragment packet
show ipv6 icmp6state	Show the ICMPv6 statistics information
show ipv6 interface	Show the IPv6 information of the interface
show ipv6 interface statistics	Show the IPv6 statistics information of the interface
show ipv6 max-mtu	Show the IPv6 MTU maximum value supported by the system
show ipv6 mtu	Show the MTU information of the IPv6 path
show ipv6 neighbors	Show the IPv6 neighbor information
show ipv6 prefix	Show the IPv6 address prefix information
show ipv6 sockets	Show the IPv6 socket information
show ipv6 statistics	Show the IPv6 basic statistics information
show ipv6 tcp syncache detail	Show the syncache entry information of the IPv6 TCP protocol
show ipv6 tcp syncache statistics	Show the syncache statistics information of the IPv6 TCP protocol
show ipv6 tcp6state	Show the IPv6 TCP statistics information
show ipv6 udp6state	Show the IPv6 UDP statistics information

5.5.3 IPv6 Basic Configuration Example

5.5.3.1 Configure the IPv6 Address of the Interface

Network Requirements

- Two devices are connected via the Ethernet port, configure the IPv6 global unicast address for the interface, and verify the connectivity between them.

Network Topology

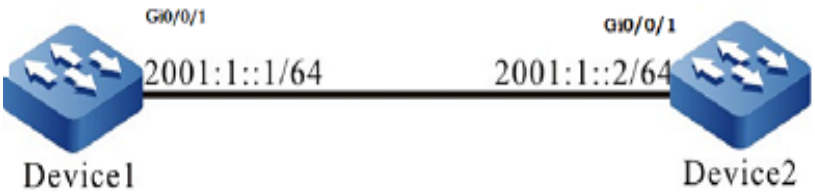


Figure 79 Networking for configuring the Ipv6 address of the interface

Configuration Steps

Step 1: Enable the IPv6 forwarding capability of the device.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 unicast-routing
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 unicast-routing
```

Step 2: Configure the global unicast address of the interface.

#Configure the global unicast address of Device1 interface gigabitethernet0/0/1 as 2001:1::1/64.

```
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 address 2001:1::1/64
Device1(config-if-gigabitethernet0/0/1)#exit
```

#Configure the global unicast address of Device2 interface gigabitethernet0/0/1 as 2001:1::2/64.

```
Device2(config)# interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 address 2001:1::2/64
Device2(config-if-gigabitethernet0/0/1)#exit
```

Step 3: Check the result.

#View the Device1 interface information.

```
Device1#show ipv6 interface gigabitethernet0/0/1
gigabitethernet0/0/1 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 configuring the IPv6 address, enable the IPv6 protocol function on the interface automatically, generate the local address of the link automatically, and add into the corresponding multicast group.

```
#View the interface information of Device2.
Device2#show ipv6 interface gigabitethernet0/0/1
gigabitethernet0/0/1 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)
#Ping the link local address of Device2 fe80::0201:7aff:fe22:e222 on Device1.
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: gigabitethernet0/0/1
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/96/483 ms.
```

Note

- When pinging the link local address, it is necessary to specify the egress interface, which is the interface on the same link of the ping link local address.

```
#On Device1, ping the global unicast address of Device2 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 can ping each other.
```

5.5.3.2 Configure IPv6 Neighbor Discovery

Network Requirements

- Device and PC belong to one LAN.
- Configure the interface of Device gigabitethernet0/0/1 with the EUI-64 address.
- PC gets the IPv6 address prefix via the IPv6 neighbor discovery protocol, configure the IPv6 address according to the got address automatically. Realize the communication of the IPv6 protocol between PC and Device.

Network Topology

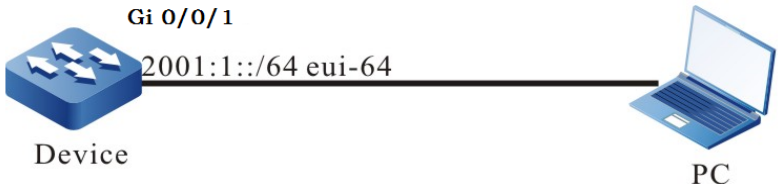


Figure 80 Networking for configuring IPv6 neighbor discovery

Configuration Steps

Step 1: Enable the IPv6 forwarding capability of the device.

```
Device#configure terminal
Device(config)#ipv6 unicast-routing
```

Step 2: Configure the EUI-64 unicast address, and enable the RA advertising function.

#Configure Device gigabitethernet0/0/1 with the EUI-64 address, and enable the RA advertising function of gigabitethernet0/0/1.

```
Device(config)#interface gigabitethernet0/0/1
Device(config-if-gigabitethernet0/0/1)#ipv6 address 2001:1::/64 eui-64
Device(config-if-gigabitethernet0/0/1)#no ipv6 nd suppress-ra period
Device(config-if-gigabitethernet0/0/1)#no ipv6 nd suppress-ra response
Device(config-if-gigabitethernet0/0/1)#exit
```

Note

- By default, the RA advertising function is disabled.

#View the interface information of Device.

```
Device#show ipv6 interface gigabitethernet0/0/1
gigabitethernet0/0/1 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)
  ND config flags is 0x0
  ND MaxRtrAdvInterval is 600
  ND MinRtrAdvInterval is 198
  ND AdvDefaultLifetime is 1800"
```

Step 3: Configure PC.

#On the PC, install the Ipv6 protocol. The Ipv6 configuration depends on the operation system. This text takes Windows XP as an example to describe.

```
C:\>ipv6 install
Installing...
Succeeded.
```

Step 4: Check the result.

```
#View the PC interface information.
C:\>ipconfig
.....(some displayed information is omitted)
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
```

You can see that the PC gets the Ipv6 address prefix 2001:1::/64, and generates the global unicast address according to the prefix automatically.

Note

- After the Windows XP host gets the address prefix, it generates two global unicast addresses. The interface ID of one address is generated according to the MAC address of the interface, and the interface ID of the other address is generated randomly.

#On Device, ping the link local address of the PC 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: gigabitethernet0/0/1
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/29/149 ms.
```

#On Device, ping the auto generated global unicast address 2001:1::15b3:d4:f13d:c3da and 2001:1::3a83:45ff:feef:c724 on the 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 can ping each other.

Note

- When pinging the link local address, it is necessary to specify the egress

interface, which is the interface on the same link of the ping link local address.

5.6 DHCPv6

5.6.1 Overview

It is hard to manage a large network. For example, in a network in which IPv6 addresses are manually allocated, IPv6 address conflicts are common. The only way of solving the problem is to dynamically allocate IPv6 addresses to the hosts. The Dynamic Host Configuration Protocol (DHCPv6) allocates IPv6 address to requesting hosts from an address pool. DHCPv6 also provides other information, such as DNS server address. DHCPv6 reduces the workload of the administrator in recording and tracking manually allocated IPv6 addresses.

DHCPv6 is a protocol that is based on UDP broadcast. The process for a DHCPv6 client to obtain an IPv6 address and other configuration information contains four phases:

SOLICT phase. When the DHCPv6 client logs into the network for the first time, it sends a DHCP SOLICT packet, whose source address is the linklocal address of the client and destination address is ff02::1:2.

ADVERTISE phase. After the DHCPv6 server receives the DHCP SOLICT broadcast packet sent by the client, it selects an IPv6 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 ADVERTISE 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.

REPLY phase. After the DHCPv6 server receives the DHCPv6 REQUEST packet from the DHCPv6 client, it sends a DHCP ACK message containing the provided IPv6

address and other configuration to the DHCPv6 client, telling the DHCPv6 client that the DHCPv6 client can use the provided IPv6 address.

The IPv6 address that the DHCPv6 server allocates to the DHCPv6 client has a lease. After the lease expires, the DHCPv6 server will take back the allocated IPv6 address. When the lease term of the IPv6 address of the DHCPv6 client has passed half time, the DHCPv6 client sends a DHCP ENEW packet to the DHCPv6 server requesting to update its IPv6 address lease. If the DHCPv6 client can continue to use the IPv6 address, the DHCPv6 server responds with a DHCP REPLY packet, requesting the DHCPv6 client to update the lease. If the DHCPv6 DHCP client cannot to continue to use the IPv6 address, the DHCPv6 server does not respond.

During dynamic IPv6 address acquisition, request packets are sent in broadcast mode; therefore, DHCPv6 is applied only when the DHCPv6 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 IPv6 address through the DHCPv6 server, the hosts of the subnets communicate with the DHCPv6 server through a DHCPv6 relay to obtain IPv6 addresses and other configuration information.

5.6.2 DHCPv6 Function Configuration

Table 476 DHCPv6 Function List

Configuration Tasks	
Configure a DHCPv6 address pool	Create a DHCPv6 address pool
	Configure an IPv6 address range
	Configure a DNS server address
	Configure the lease of an IPv6 address
	Configure IPv6 to bind with DUID and IAID
Configure other parameters of a DHCPv6 server	Configure the DHCPv6 server
	Configure the range of reserved IPv6 addresses
	Configure DHCPv6 ping detection parameters.
	Configure the lease update of the DHCP address pool

	Configure the data log function of the DHCPv6 server
Configure the functions of a DHCPv6 client	Configure a DHCPv6 client
	Configure the DHCPv6 Option 16 function
Configure the DHCPv6 relay function	Configure a DHCPv6 relay.
	Configure the source address of the DHCPv6 relay packet
	Configure the DHCPv6 server address
	Configure the DHCPv6 interface-id option

5.6.2.1 Configure a DHCPv6 Address Pool

Configuration Condition

None

Create a DHCPv6 Address Pool

A DHCPv6 server needs to select and allocate IPv6 addresses and other parameters from a DHCPv6 address pool. Therefore, a DHCPv6 address pool must be created for the DHCPv6 server.

Table 477 Creating a DHCPv6 Address Pool

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create one DHCPv6 address pool and enter the DHCPv6 configuration mode	ipv6 dhcp pool *pool-name*[vrf *vrf-name*]	Mandatory By default, the system does not create the DHCPv6 address pool.

Note

- Address pools fall into two types: Network and Range. The two types of

address pools can be configured respectively through the network and range commands.

Configure an IPv6 Address Range

On a DHCPv6 server, each DHCPv6 address pool must be configured with an IPv6 address range to allocate IPv6 addresses to DHCPv6 clients.

Table 478 Configuring an IPv6 Address Range

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCPv6 configuration mode	ipv6 dhcp pool *pool-name*[vrf *vrf-name*]	-
Configure an IPv6 address range for an address pool of the Network type.	network *ipv6-address/prefix-length*	Optional. By default, an IPv6 address range is not configured for an address pool.
Configure an IPv6 address range for an address pool of the Range type.	range *low-ipv6-address high-ipv6-address prefix-length*	Optional. By default, an IPv6 address range is not configured for an address pool.

Note

- Modify the type of the address pool from network to range (or from range to network). If the new address range intersects with the old address range, the command line will prompt the user whether to perform the operation. If yes, it will delete the address configuration (static binding) and dynamic lease related to the address pool; if the actual effective range of the new address includes the actual effective range of the old address, the address pool reserves the relevant address configuration (static binding) under the

address pool. But dynamic leases are deleted.

Configure a DNS Server Address

On a DHCPv6 server, you can configure the DNS server address respectively for each DHCPv6 address pool. When a DHCPv6 server allocates an IPv6 address for a DHCPv6 client, it also sends the DNS server address to the client.

When the DHCPv6 client starts dynamic domain name resolution, it queries the DNS server.

Table 479 Configuring a DNS Server Address

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the DHCPv6 configuration mode	ipv6 dhcp pool *pool-name*[vrf *vrf-name*]	-
Configure a DNS server address	dns-server { *ipv6-address*&<1-8> | autoconfig }	Mandatory. By default, the DNS server address is not configured.

Configure the Lease of an IPv6 Address

The IPv6 address that the DHCPv6 server allocates to the DHCPv6 client has a lease. After the lease expires, the server will take back the allocated IPv6 address. If the DHCPv6 client wants to continue to use the IPv6 address, it must have the IPv6 address lease updated.

On the DHCPv6 server, you can configure an IPv6 address lease for each DHCPv6 address pool.

Table 480 Configuring the Lease of an IPv6 Address

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

Enter the DHCPv6 configuration mode	ipv6 dhcp pool *pool-name*[vrf *vrf-name*]	-
Configure the lease of the IPv6 address	lease preferred-lifetime *preferred-lifetime* valid-lifetime *valid-lifetime*	Mandatory By default, the preferred-lifetime is 604800 (sevent days), and valid-lifetime is 2592000s (30 days).

Configure IPv6 to Bind with DUID, IAID

Configure IPv6 to bind with client DUID and IAID. When specifying the client of DUID and IAID to request for allocating the IPv6 address to the DHCPv6 server, the DHCPv6 server will allocate the IPv6 address it binds to. As long as the DIID and IAID of the client remain unchanged, the IPv6 address acquired by the client from the server is the same every time.

Table 481 Configure Ipv6 to bind with DUID, IAID

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the 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* | decimal *iaid*}]	Mandatory By default, do not configure IPv6 to bind with DUID, IAID.

Note

- The command is valid only for the Range and Network address pools.
- When configuring the static binding of the same duid and iaid, the address pool permits binding five IPv6 addresses.

- When the configured static binding only specifies duid, not specifying iaid, the address pool only permits binding one IPv6 address.

5.6.2.2 Configure Other Parameters of a DHCPv6 Server

Configuration Condition

None

Configure DHCPv6 Server

After configuring the interface to work in the DHCPv6 server mode, the DHCPv6 server will distribute the IPv6 address and other network parameters to the client when the interface receives the DHCPv6 request packet from the DHCPv6 client.

Table 482 Configure the DHCPv6 server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the DHCPv6 server	ipv6 dhcp server	Mandatory By default do not configure the DHCPv6 server.

Configure the Range of Reserved IPv6 Addresses

In a DHCPv6 address pool, some IPv6 addresses are reserved for some special devices, and some IPv6 addresses conflict with the IPv6 addresses of other hosts in the network. Therefore, the IPv6 addresses cannot be dynamically allocated.

Table 483 Configure the Range of Reserved IPv6 Addresses

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the range of reserved	ipv6 dhcp excluded-address	Mandatory.

IPv6 addresses.	*low-ipv6-address* [*high-ipv6-address*] [vrf *vrf-name*]	By default, the range of reserved IPv6 addresses is not configured. The IPv6 addresses in the reserved IP address range will not be allocated.

Configure DHCPv6 Ping Detection Parameters

To prevent an IPv6 address conflict, before dynamically allocating an IPv6 address to a DHCPv6 client, a DHCPv6 server must detect the IPv6 address. The detection operation is performed through the ping operation. The DHCPv6 server determines whether an IPv6 address conflict exists by checking whether an ICMP echo response packet is received within the specified time.

Table 484 Configuring DHCPv6 Ping Detection Parameters

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure DHCPv6 ping detection parameters	ipv6 dhcp ping { packets *packet-num* | timeout *milliseconds* }	Mandatory. By default, the number of ping packets is 1, and the timeout time is 50 ms.

Configure Lease Update of DHCPv6 Address Pool

Configure the lease update time of the DHCPv6 server, and the lease information formed by the address pool on the DHCPv6 server will be written to the file.

Table 485 Configure lease update time of DHCPv6 address pool

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the lease update interval of the DHCPv6 server	ipv6 dhcp server database update {now| internal *seconds*}	Mandatory By default, the lease is updated every 3600s.

Configure the Data Log Function of the DHCPv6 Server

After enabling the data log function of the DHCPv6 server, the distribution of the address pool on the DHCPv6 server is recorded in the data log.

Table 486 Configuring the Data Log Function of the DHCPv6 Server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the data log function of the DHCPv6 server	ipv6 dhcp logging security-data	Mandatory By default, do not enable the data log function.

5.6.2.3 Configure the Functions of a DHCPv6 Client

Configuration Condition

None

Configure a DHCPv6 Client

The interface of the DHCPv6 client obtains an IPv6 address and other parameters through DHCP.

Table 487 Configuring a DHCPv6 Client

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the DHCPv6 client to obtain an IPv6 address	ipv6 dhcp client address [rapid-commit]	Mandatory. By default, the DHCPv6 client is not configured to obtain an IPv6 address.
Configure the DHCPv6 client to get the IPv6 prefix	ipv6 dhcp client pd *pool-name* [rapid-commit]	Mandatory By default, do not configure the DHCPv6 client to get the IPv6

		prefix.

5.6.2.4 Configure the Function of a DHCPv6 Relay

Configuration Condition

None

Configure a DHCPv6 Relay

If multiple subnets exist in a network and the hosts of the subnets need to obtain configuration information such as IPv6 address through the DHCPv6 server, the hosts of the subnets communicate with the DHCPv6 server through a DHCPv6 relay to obtain IPv6 addresses and other configuration information. If an interface is configured to work in DHCPv6 relay mode, after the interface receives DHCPv6 packets from a DHCPv6 client, it relays the packet to the specified DHCPv6 server. The DHCPv6 server then allocates an IP address.

Table 488 Configuring a DHCPv6 Relay

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the DHCPv6 relay function	ipv6 dhcp relay	Mandatory By default, do not configure the DHCPv6 relay function.

Configure Source Address of DHCPv6 Relay

DHCPv6 relays the DHCPv6 client to the source address of the server packet. By default, use the address of the egress interface of the route to the DHCPv6 server. In some special environment, the DHCPv6 server cannot communicate with the address. Therefore, users can configure the source address of the DHCPv6 relay packet to the DHCPv6 server and the LinkAddr field in the packet through the **ipv6 dhcp relay source-address** command.

Table 489 Configure the source address of the DHCPv6 relay packet

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the source address of the DHCPv6 relay	ipv6 dhcp relay source-address *ipv6-address*	Mandatory By default, do not configure the source address of the DHCPv6 relay packet.

Configure the Address of the DHCPv6 Server

When the interface receives the DHCPv6 packet sent by the DHCPv6 client, relay the packet to the configured DHCPv6 server, which distributes the IPv6 address.

Table 490 Configure the address of the DHCPv6 server

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the address of the DHCPv6 server	ipv6 dhcp relay server -address *ipv6-address*	Mandatory By default, do not configure the address of the DHCPv6 server.

Configure DHCPv6 interface-id Option

The command is used to configure the interface-id option supported by DHCPv6 relay.

Table 491 Configure DHCPv6 server address

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the DHCPv6	ipv6 dhcp relay interface –id [	Mandatory

interface-id option	interface]	By default, do not configure the filling mode of interface-id option.

5.6.2.5 DHCPv6 Monitoring and Maintaining

Table 492 DHCPv6 Monitoring and Maintaining

Command	Description
clear ipv6 dhcp pool *pool-name* { lease | conflict [*ipv6-address*] }	Clear the dynamic lease information or conflict address information in the address pool
clear ipv6 dhcp server interface [*interface-name*] statistics	Clear the key information statistics when the DHCPv6 server interacts packets with the client or relay
clear ipv6 dhcp relay statistics	Clear the statistics information on the DHCPv6 relay device
show ipv6 dhcp server interface *interface-name* [statistics]	Display the associated address pool information in the specified interface or display the key information statistics when the DHCPv6 server in the specified interface interacts packets with the client or relay
show ipv6 dhcp pool *pool-name* { summary | ping_list | offer_list | excluded_list | conflict_list | lease | binding }	Display the summary information of the specified address pool or the address information of the ping check or the information about the address that has sent OFFER packet and is waiting for DHCPv6 client to reply the REQUEST packet or display the exclude address information in the address pool or display the conflict address information in the address pool or display the dynamic lease information in the address pool or display the static

	binding information in the address pool.
show ipv6 dhcp pool *pool-name* specific { ipv6-address *ipv6-address* | duid *duid* }	Display the specified ipv6 address or client DUID information in the address pool
show ipv6 dhcp relay [interface *interface-name*]	Display the packet statistics information on the DHCPv6 relay device

5.6.3 DHCPv6 Typical Configuration Example

5.6.3.1 Configure a DHCPv6 Server to Statically Allocate IPv6 Addresses

Network Requirements

- Device2 acts as a DHCPv6 server to allocate IPv6 addresses and DNS server IPv6 addresses in a static manner.
- The DHCPv6 server allocates an IP address to PC1 in DUID binding mode, and allocates an IPv6 address to PC2 in the DUID+IAID binding mode.

Network Topology

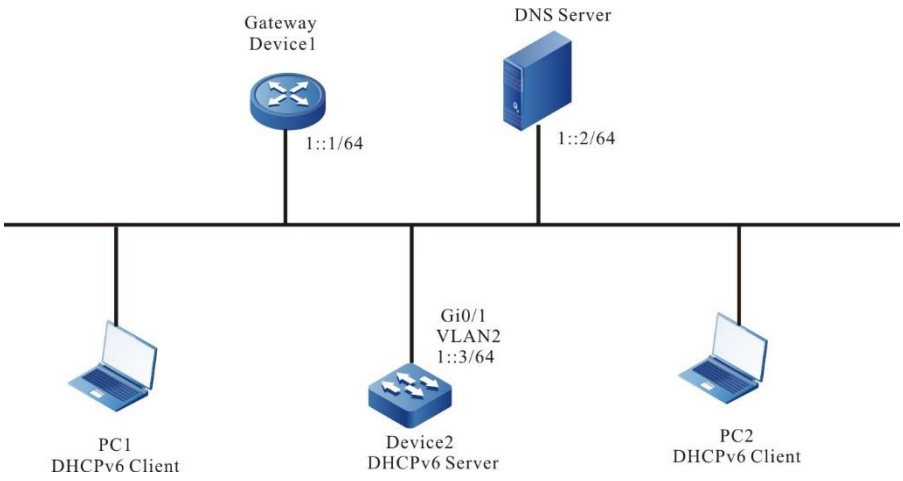


Figure 81 Configuring a DHCPv6 Server to Statically Allocate IPv6 Addresses

Configuration Steps

Step 1: Configure the IPv6 address of the Device2 interface and the 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 the static binding address pool and parameters.

#Configure the address pool binding, and adopt the DUID binding mode to distribute IPv6 address for PC1. Adopt the static DUID+IAID binding mode to distribute the IPv6 address for PC2.

```
Device2(config)#ipv6 dhcp pool binding
Device2(dhcp6-config)#bind                    1::11                    duid
00020000161330303031376163663564663 4
Device2(dhcp6-config)#bind                    1::12                    duid
00020000161363636438316631303761623 9 iaid 00010071
Device2(dhcp6-config)#dns-server 1::2
Device2(dhcp6-config)#exit
```

Step 3: Check the result.

#Check the association of the server interface and address.

```
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 the static binding of the server.

```
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, query the IPv6 addresses distributed for PC1 and PC2 via the **show ipv6 dhcp pool binding lease** command.

```
Device2#show ipv6 dhcp pool mac-binding lease
IPv6 Address          Duid                                laid     Type     Time Left(s) ---
--------- ------------------------------------     --------  -------  --
----------
1::11       000200001613303030313761636635646634       00000000    Lease
2591974
1::12       000200001613636364383166313037616239       00010071    Lease
2591974
```

On PC1 and PC2, check whether the got IPv6 addresses and the IPv6 address of the DNS server are correct.

5.6.3.2 Configure a DHCPv6 Server to Dynamically Allocate IPv6 Addresses

Network Requirements

- Two interface VLANs of Device, VLAN2 and VLAN3, are respectively configured with IPv6 addresses 1::3/64 and 2::3/64.
- The DHCPv6 server Device dynamically allocates IPv6 addresses 1::/64 and 2::/64 to the two clients in the directly-connected physical network.
- The addresses in network segment 1::/64 have a one-day lease, the DNS server address is 2::4. The addresses in network segment 2::/64 have a three-day lease the gateway address is 2::3, the DNS server address is 2::4.
- The first 10 IPv6 addresses in network segments 1::/64 and 2::/64 are reserved and cannot be allocated.

Network Topology

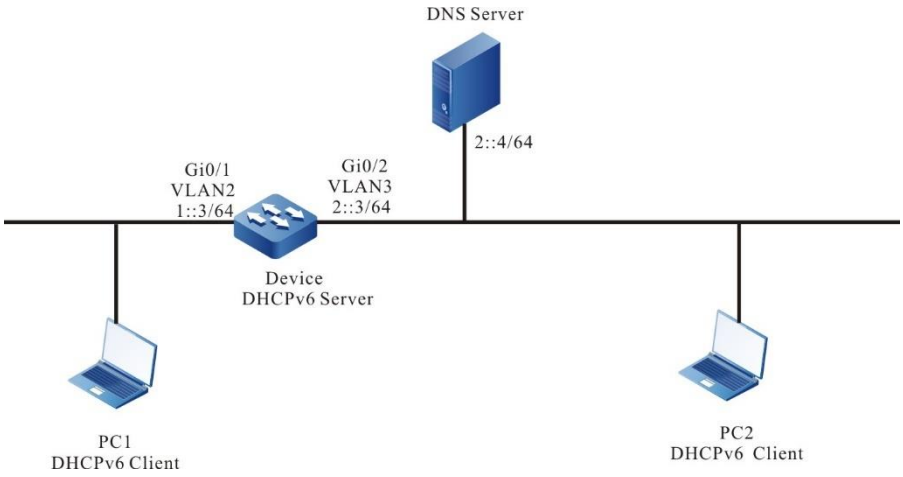


Figure 82 Configuring a DHCPv6 Server to dynamically Allocate IPv6 Addresses

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. Configure the IPv6 address of the interface (omitted).

Step 2: On the DHCPv6 server Device1, configure two dynamic address pools and their parameters.

#Configure the 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 the first 10 IP addresses in the two address pools to be reserved.

```
Device(config)#ipv6 dhcp excluded-address 1::0 1::9
Device(config)#ipv6 dhcp excluded-address 2::0 2::9
```

#Configure address pool dynamic-pool1 and its parameters (including address range, DNS address, address lease).

```
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 address pool dynamic-pool2 and its parameters (including address

range, DNS address, address lease).

```
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.

#On Device, query the IPv6 addresses that are allocated to clients.

```
Device#show ipv6 dhcp pool dynamic-pool1 lease
IPv6 Address          Duid                    Iaid    Type     Time Left(s)
------------    ----------------------------    -------- -------  ------------
1::a        00020000161330303031376163635646634  00000000  Lease      86390
Device2#show ipv6 dhcp pool dynamic-pool2 lease
IPv6 Address       Duid                    Iaid       Type     Time Left(s)
------------   --------------------------    --------   -------   ------------
2::a       00020000161330303031376163635646634 00000000   Lease      2591974
```

On the DHCPv6 clients, query whether the IPv6 addresses have been obtained properly.

Caution

- The IPv6 addresses in the address pool must be within the network segment range of the interface that provides the service.

5.6.3.3 Configure DHCPv6 Relay

Network Requirements

- Device1 is the DHCPv6 server, and the interface of Device2 enables the DHCPv6 relay function.
- The DHCPv6 server provides the service for the client of the segment 1::/64, and the first ten IPv6 addresses are reserved.
- The DHCPv6 client gets the IPv6 address via DHCPv6 relay.

Network Topology

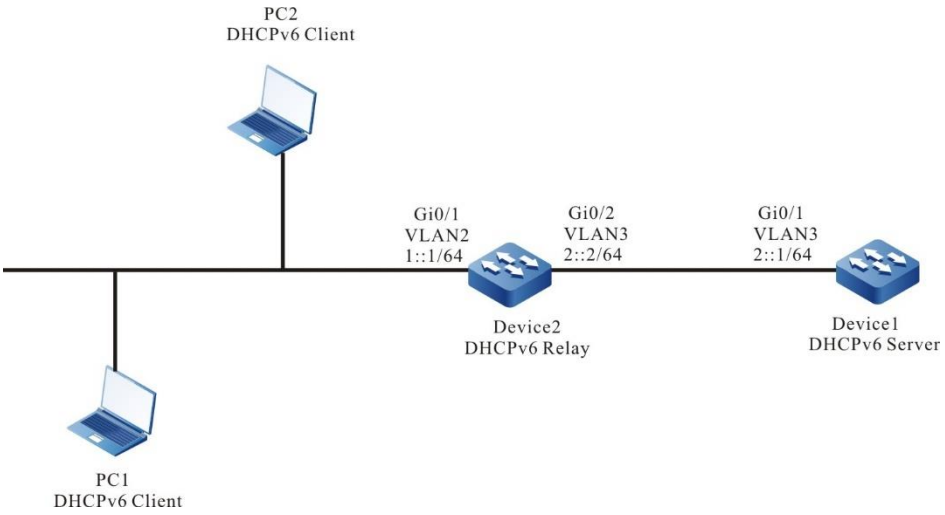


Figure 83 Networking for Configuring a DHCPv6 Relay

Configuration Steps

Step 1: Create VLANs, and add ports to the required VLANs. Configure the IPv6 address of the interface (omitted).

Step 2: Configure an IPv6 address pool for Device 1, and configure the 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 IPv6 addresses which are from 1::0 to 1::9 not to be allocated.

```
Device1(config)#ipv6 dhcp excluded-address 1::0 1::9
```

#Configure IPv6 address pool dynamic-pool for Device1.

```
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 a static route to network segment 1::/64.

```
Device1(config)#ipv6 route 1::0/64 2::2
```

Step 3: On the interface vlan2 of Device2, enable the DHCPv6 relay and configure the address of the DHCPv6 server 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
```

Step 4: Check the result.

#On Device1, query the IPv6 addresses that have been allocated.

```
Device1#show ipv6 dhcp pool dynamic-pool lease
IPv6 Address            Duid                                 Iaid     Type    Time Left(s)
------------  ----------------------------------     --------  -------  ------------
1::0          00020000161330303031376163663564634      00000000   Lease     574
```

Use the **show ipv6 dhcp pool dynamic-pool lease** command to query the IPv6 addresses that have been allocated to clients. The result shows that a client has obtained the IPv6 address 1::0.

5.7 GRE

5.7.1 Overview

Generic Routing Encapsulation (GRE) is a generic tunnel encapsulation protocol which defined how to use a network protocol to encapsulate another network protocol.

GRE tunnel is one tunnel technology among a lot of tunnel technologies. The starting point and end point of a tunnel need to be manually configured. The tunnel is a virtual end-to-end connection. It provides a transmission channel for the encapsulated packets. The two ends of the tunnel encapsulate and de-capsulate data packets respectively.

- GRE encapsulation:

If a data packet needs to be transmitted through a GRE tunnel, the tunnel adds a GRE header to the packet header, and adds an IP header to the GRE header. Set the protocol number of the IP header to 47 (GRE protocol number in the IP header), set the source address of the IP header to the source address of the tunnel, and set the destination address of the IP header to the destination address of the tunnel.

- GRE packet structure

Delivery header	GRE header	Payload packet

Payload packet: The network layer packet (such as IP packet) before it enters the tunnel is taken as the valid payload of the tunnel packet. The protocol of the packet is called the passenger protocol of the GRE tunnel.

GRE header: It refers to the GRE header that is added to the payload packet after the payload packet enters the tunnel. The GRE header contains the GRE protocol and some information related to the passenger protocol.

Delivery header: The encapsulated external protocol header (such as IP header) is the header of the protocol for the network in which the tunnel is located. It is a transmission tool which helps one protocol packet to traverse the network of another protocol.

- GRE packet forwarding

After a packet is encapsulated at the starting point of a GRE tunnel, it selects a route according to the destination after encapsulation, and then it is sent out through the corresponding network interface. Intermediate devices take the packet as a common packet until the packet reaches the end of the tunnel.

- GRE decapsulation:

Decapsulation is the reverse process of encapsulation. After the end point of the tunnel receives the packet, it analyzes Delivery header. If the end point of the tunnel finds that the destination is its own address, it checks the protocol field of the IP header. If the protocol field is 47 (GRE protocol number), the end point of the tunnel hands over the packet to the GRE tunnel for processing. The tunnel first removes Delivery header and then checks the protocol number, checksum, and keyword in the GRE header. After required processing, the tunnel removes the GRE header, and hands over the Payload packet to the passenger protocol for later processing. Then, the decapsulation is completed.

5.7.2 GRE Function Configuration

Table 10-493 GRE function list

Configuration Tasks	
Configure a GRE tunnel.	Configure a GRE over IPv4 tunnel.
	Configure a GRE over IPv6 tunnel.

5.7.2.1 Configure a GRE Tunnel

Configuration Condition

Before configuring a GRE tunnel, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Tunnel interfaces have been created and the basic parameters have been configured. (Refer to tunnel interface configuration manual.)
- A unicast protocol has been configured so that the routes at the two ends of the tunnel are reachable.

Configure a GRE Tunnel

Table 10-494 Configuring a GRE tunnel

Step		Command	Description
Enter the global configuration mode.		configure terminal	-
Enter the tunnel interface configuration mode.		interface tunnel *tunnel-number*	-
Configure the tunnel interface address.	Configure IPv4 unicast address	ip address *ip-address* { *mask* | *mask-length* }	Mandatory. By default, no address is configured for the tunnel interface.
	Configure the	ipv6 address { *ipv6-*	

Step		Command	Description
	IPv6 global unicast address or anycast address or local address of the site or auto get address	*address/prefix-length* [anycast | eui-64] | autoconfig }	
	Configure the local address of the IPv6 link	ipv6 address *IPv6-address* link-local	Optional By default, after the interface enables IPv6, generate the local address of the link automatically.
Configure the tunnel interface mode to GRE over IPv4 or GRE over IPv6		tunnel mode gre [ip | ipv6]	Optional. By default, the tunnel interface mode is GRE over IPv4.
Configure the source address or interface name on the tunnel interface.		tunnel source { *ip-address* | *ipv6-address* | *interface-name* }	Mandatory. By default, the source address and interface name are not configured on the tunnel interface.
Configure the destination address or host name on the tunnel interface.		tunnel destination { *ip-address*| *ipv6-address* }	Mandatory. By default, the destination address is not configured on the tunnel interface.

Note

- On the two end of a tunnel, the source addresses and destination addresses must be configured. The source address of one end is the destination end of the other end.
- In configuring the source of a tunnel, if the interface mode is adopted, the primary address of the source interface is used as the source address of the tunnel.
- The two ends of a tunnel must be configured with the same tunnel mode; otherwise, transmission through the tunnel fails.
- Two or more tunnels with the same tunnel mode, source address and destination address cannot be configured on the same device at the same time.

5.7.2.2 GRE Monitoring and Maintaining

Table 10-495 GRE monitoring and maintaining

Command	Description
enable	Privileged mode
debug tunnel {all | config | event | forward| packet }	Open the switch of the Tunnel debug information
show tunnel [*tunnel-id*] [*slot slot-num*]	Display the tunnel information

5.7.3 GRE Typical Configuration Example

5.7.3.1 Configure GRE Basic Functions

Network Requirements

- IP Network1 and IP Network2 are two private networks of Device1 and

Device3.

- IP Network1 and IP Network2 communicate with each other through the GRE tunnel between Device1 and Device3.

Network Topology

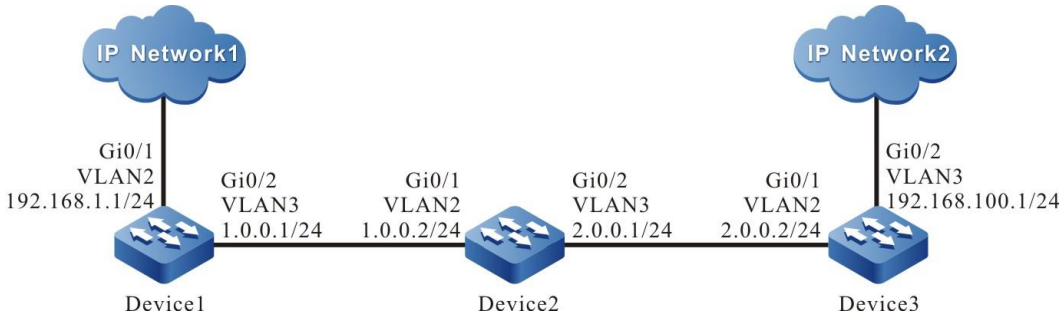


Figure 84 Networking for configuring GRE basic functions

Configuration Steps

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

Step 2: Configure IP addresses for all interfaces. (Omitted)

Step 3: Configure Open Shortest Path First (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)#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)#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)#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

O   1.0.0.0/24 [110/65536] via 2.0.0.1, 00:18:40, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:22:27, gigabitethernet0
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
```

Note

- The method for querying the routing table of Device 1 and Device2 is the same as that for Device 3, so the processes are not described here.

Step 3: Configure a GRE tunnel.

#On Device1, configure GRE tunnel tunnel1, set the source address to 1.0.0.1, destination address to 2.0.0.2, and IP address to 10.0.0.1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#exit
```

#On Device3, configure GRE tunnel tunnel1, set the source address to 2.0.0.2, destination address to 1.0.0.1, and IP address to 10.0.0.2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#exit
```

#Query the GRE tunnel information of Device3.

```
Device3#show tunnel 1
```

```
Tunnel 1:
   Tunnel mode is gre ip
      Gre checksum validation is disabled
      Gre key is not set
      Gre keepalive is disabled
   Source ipv4 address is 2.0.0.2 (Source ipv4 address is up on source interface gigabitethernet0)
   Destination ipv4 address is 1.0.0.1
   Tunnel state is up
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Note

- The method for querying the GRE tunnel information of Device 1 is the same as that for Device 3, so the process is not described here.
- If a tunnel is located at different network segments, both the two devices at the two ends of the tunnel must be configured with a static route that reaches the peer tunnel with the tunnel interface as the output interface.

Step 4: Configure the static route.

#On Device1, configure the static route to the egress interface tunnel1 of IP Network2.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device3, configure the static route to the egress interface tunnel1 of IP Network1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#View the route 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 [110/65536] via 2.0.0.1, 00:43:30, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:47:17, gigabitethernet0
C   10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S   192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
```

Note

- The method for querying the routing table of Device 1 is the same as that for Device 3, so the process is not described here.

5.7.3.2 Configure GRE over IPv6 Basic Functions

Network Requirements

- IP Network1 and IP Network2 are the private IP networks of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 are the private IPv6 networks of Device1 and Device3 respectively.
- IP Network1 and IP Network2 communicate with each other through the GRE over IPv6 tunnel between Device1 and Device3.
- IPv6 Network1 and IPv6 Network2 communicate with each other through the GRE over IPv6 tunnel between Device1 and Device3.

Network Topology

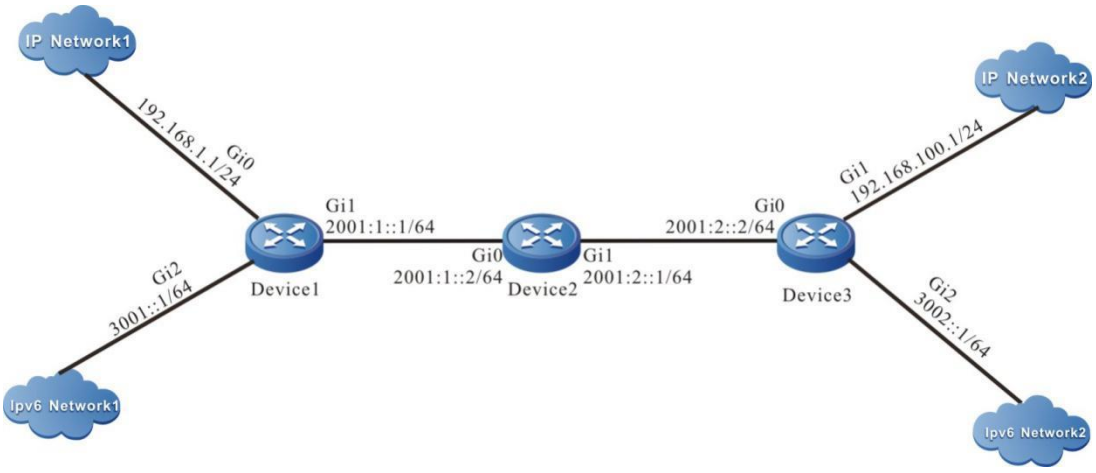


Figure 85 Networking of configuring GRE over IPv6 basic functions

Configuration Steps

Step 1: Configure IP addresses for all interfaces. (Omitted)

Step 2: Configure OSPFv3, making Device1, Device2, Device3 be able to communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.75.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ipv6 router ospf tag 100 area 0
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id  1.2.75.1
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 router ospf tag 100 area 0
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ipv6 router ospf tag 100 area 0
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3.

```
Device3#configure terminal
```

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 1.1.73.1
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ipv6 router ospf tag 100 area 0
Device3(config-if-gigabitethernet0)#exit
```

#View the IPv6 route 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 ::, 6w0d:23:09:31, lo0
O   2001:1::/64 [110/2]
     via fe80::508b:fff:fee4:ff6, 00:08:37, gigabitethernet0
C   2001:2::/64 [0/0]
     via ::, 00:15:51, gigabitethernet0
L   2001:2::2/128 [0/0]
     via ::, 00:15:50, lo0
C   3002::/64 [0/0]
     via ::, 00:15:06, gigabitethernet2
L   3002::1/128 [0/0]
     via ::, 00:15:04, lo0
```

Note

- The method for querying the routing table of Device 1 and Device2 is the same as that for Device 3, so the processes are not described here.

Step 3: Configure GRE over IPv6 tunnel.

#Configure GRE over IPv6 Tunnel 1 on Device1, the source address is 2001:1:: 1, the destination address is 2001:2:: 2, the IP address is 10.0.0.1, and the IPv6 address is 10:: 1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode gre IPv6
```

```
Device1(config-if-tunnel1)#tunnel source 2001:1::1
Device1(config-if-tunnel1)#tunnel destination 2001:2::2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#Configure GRE over IPv6 Tunnel 1 on Device3 with source address of 2001:2:: 2, destination address of 2001:1:: 1, IP address of 10.0.0.2 and IPv6 address of 10:: 2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode gre IPv6
Device3(config-if-tunnel1)#tunnel source 2001:2::2
Device3(config-if-tunnel1)#tunnel destination 2001:1::1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#View the GRE tunnel information of Device3.

```
Device3#show tunnel 1


Tunnel 1:
   Tunnel mode is gre ipv6
      Gre checksum validation is disabled
      Gre key is not set
   Source ipv6 address is 2001:2::2(Source ipv6 address is up on source interface gigabitethernet0)
   Destination ipv6 address is 2001:1::1
   Tunnel state is up
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Note

- The viewing method of Device1 is the same as that of Device3, and the viewing process is omitted.
- When the tunnel is not in the same network segment, the static route to the peer end tunnel needs to be configured on the devices at both ends of the tunnel, and the egress interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to the egress interface of IP Network2 tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device1, configure the static route to the egress interface of IPv6 Network2 tunnel1.

```
Device1(config)#IPv6 route 3002::/64 tunnel1
```

#On Device3, configure the static route to the egress interface of IP Network1 tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#On Device3, configure the static route to the egress interface of IPv6 Network1 tunnel1

```
Device3(config)#IPv6 route 3001::/64 tunnel1
```

#View the route 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   10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S   192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
#View the IPv6 route 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 ::, 6w0d:23:50:28, lo0
C   10::/64 [0/0]
    via ::, 00:12:23, tunnel1
L   10::2/128 [0/0]
```

```
    via ::, 00:12:22, lo0
O   2001:1::/64 [110/2]
    via fe80::508b:fff:fee4:ff6, 00:49:34, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 00:56:48, gigabitethernet0
L   2001:2::2/128 [0/0]
    via ::, 00:56:46, lo0
S   3001::/64 [1/100000]
    via ::, 00:00:14, tunnel1
C   3002::/64 [0/0]
    via ::, 00:56:02, gigabitethernet2
L   3002::1/128 [0/0]
    via ::, 00:56:01, lo0
```

Note

- The viewing method of Device1 is the same as that of Device3, and the viewing process is omitted.

5.8 IPIP

5.8.1 Overview

The IPIP (IPv4 over IPv4) tunnel is one of the tunnel technologies. Similar to the GRE (Generic Routing Encapsulation) tunnel, the start and end of the IPIP tunnel are manually configured. It serves a virtual PTP link and provides a transmission tunnel for the encapsulated packet. The start and end of the tunnel encapsulate and decapsulated the data packet. The IPIP tunnel encapsulates only the IPv4 data packets and enables the encapsulated data packets to be transmitted over other IPv4 network.

- IPIP encapsulation

When the IP data packet is transmitted over the IPIP tunnel, the tunnel adds an IP packet header. In the IP packet header, the protocol number is set to 4, the source IP address is set to the source IP address of the tunnel, and the destination IP address is set to the destination IP address of the tunnel.

- IPIP packet structure

Outer IP header	IP header	IP Payload

IP Payload: indicates the IP packet payload before the packet entering the tunnel. It is a valid payload of the tunnel packet.

IP header: indicates the IP packet heeder before the packet entering the tunnel.

Outer IP header: indicates the encapsulated outer IP packet header. It is a transmission tool which enables the IP packet to be transmitted over another IP network.

- IPIP packet forwarding

After the packet is encapsulated at the start of the IPIP tunnel, a routing is selected for the packet based on the encapsulated destination IP address and then the packet is sent out from the corresponding network interface. The intermediate equipment forwards the packet as the common IP packet until the packet reaches the end of the tunnel.

- IPIP decapsulation

Contrary to the encapsulation process, in the decapsulation process, the end of the tunnel first analyzes the outer IP header when it receives the packet. If the destination IP address is the IP address of the end of the tunnel, check the protocol field of the IP packet header. If the protocol field is 4, transmit the packet to the IPIP tunnel for handling. The tunnel removes the outer IP header of the packet and chooses a routing for the packet based on the destination IP address of the decapsulated packet. The subsequent handling is performed based on the routing result.

5.8.2 IPIP Function Configuration

Table 496 IPIP function list

Configuration Task	
Configure the IPIP tunnel	Configure the IPIP tunnel

5.8.2.1 Configure IPIP Tunnel

Configuration Condition

Before configuring the IPIP tunnel, first complete the following tasks:

- Configure the interface IP address, enabling that the adjacent nodes on the network layer are reachable.
- Create the tunnel interface and configure the basic parameters. For details, refer to the Tunnel Interface Configuration Manual.
- Configure any unicast routing protocol, enabling the routing to the both ends of the tunnel is reachable.

Configure IPIP Tunnel

Table 497 Configure the IPIP tunnel

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the tunnel interface configuration mode	interface tunnel *tunnel-number*	-
Configure the tunnel interface IP address	ip address *ip-address* { *mask* | *mask-length* }	Mandatory By default, the IP address on the tunnel interface is not configured.
Configure the tunnel interface mode as IPv4 over IPv4	tunnel mode ipip	Mandatory By default, the tunnel interface mode is GRE over IPv4.
Configure the source IP address or the interface name for the tunnel interface	tunnel source { *ip-address* | *interface-name* }	Mandatory By default, the source IP address and the interface name are not configured for the tunnel interface.
Configure the destination IP	tunnel destination { *ip-address* }	Mandatory

Step	Command	Description
address or the host name for the tunnel interface		By default, the destination IP address is not configured for the tunnel interface.

Note

- The start and end of the tunnel must be configured with the source IP address and the destination IP address. The IP address at the start and end of the tunnel are complementary source IP address and destination IP address for each other.
- When configuring the tunnel source IP address, the source IP address of the tunnel adopts the master IP address of the source IP address if the interface mode is used.
- The start and end of the tunnel must be configured with the same tunnel mode. Otherwise, the tunnel transmission fails.
- Two or more tunnels with the same tunnel mode, source IP address, and destination IP address cannot be configured on the same device.

5.8.2.2 IPIP Monitoring and Maintaining

Table 498 The IPIP monitoring and maintaining

Command	Description
show tunnel [*tunnel-id*]	Display the configuration information of all tunnels and the specified tunnel

5.8.3 IPIP Typical Configuration Example

5.8.3.1 Configure IPIP Basic Function

Network Requirements

- IP Network1 and IP Network2 are two private networks for Device1 and Device3, respectively.
- IP Network1 communicates with IP Network2 through the IPIP tunnel between Device1 and Device3.

Network Topology

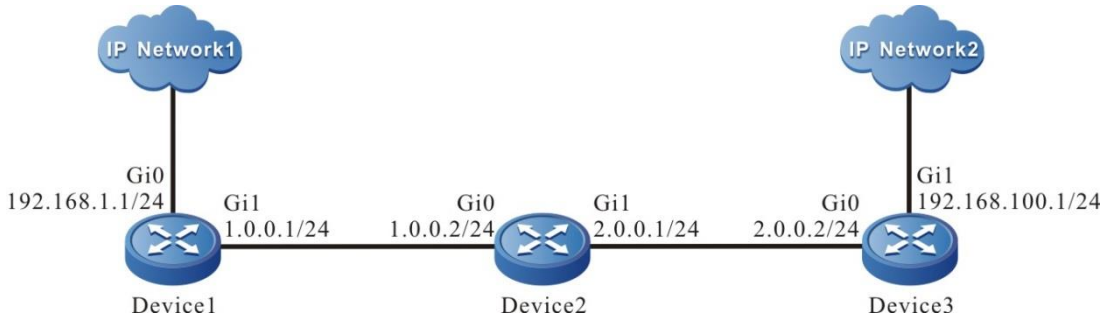


Figure 86 Networking of configuring the IPIP basic function

Configuration Steps

Step 1: Configure the IP addresses for all interfaces. (Omitted)

Step 2: Configure the 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)#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)#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)#exit
```

#View 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 [110/65536] via 2.0.0.1, 00:18:40, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:22:27, gigabitethernet0
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
```

Note

- Device1 and Device2 are viewed in the same way as Device3. The viewing process is omitted.

Step 3: Configure the IPIP tunnel.

#Configure the IPIP tunnel, tunnel1 on Device1 with source IP address as 1.0.0.1, destination IP address as 2.0.0.2, and the IP address as 10.0.0.1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipip
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#exit
```

#Configure the IPIP tunnel, tunnel1 on Device3 with source IP address as 2.0.0.2, destination IP address as 1.0.0.1, and the IP address as 10.0.0.2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipip
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#exit
#View the IPIP tunnel information of Device3.
Device3#show tunnel 1

Tunnel 1:
```

```
    Tunnel mode is ipip
    Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface
gigabitethernet0)
    Destination ipv4 address is 1.0.0.1
    Tunnel state is up
    Encapsulation vrf is global(0x0)
    TTL(time-to-live) is 255
    TOS(type of service) is not set
total(1)
```

Note

- Device1 is viewed in the same way as Device3. The viewing process is omitted.
- When the tunnel does not exist in the same network segment, devices at the both ends of the tunnel are configured with a static routing to the peer end. And the outbound interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to the egress interface tunnel1 of IP Network2.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device3, configure the static route to the egress interface tunnel1 of IP Network1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#View the route 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 [110/65536] via 2.0.0.1, 00:43:30, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:47:17, gigabitethernet0
```

```
C   10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S   192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
```

Note

- Device1 is viewed in the same way as Device3. The viewing process is omitted.

5.9 Transition Tunnel

5.9.1 Overview

The transition tunnel (IPv6 over IPv4) technology provides a way to transfer the IPv6 data with the existing IPv4 routing system: the IPv6 packet is encapsulated in the IPv4 packet as unstructured data and transmitted through the IPv4 network. According to the different setup modes, the transitional tunnels can be divided into manual tunnels and automatic tunnels. The transition tunnel technology skillfully utilizes the existing IPv4 network, its significance lies in providing a way to enable IPv6 nodes to communicate during the transition period, but it cannot solve the intercommunication problem between IPv6 nodes and IPv4 nodes. Transition tunnels are divided into manual type and automatic type. The corresponding relationship between the types and the modes is as follows:

Table 499 Transition tunnel mode

Tunnel Type	Tunnel Mode	Tunnel Source/Destination Address	Tunnel Interface Address
Manual tunnel	IPv6 over IPv4 manual tunnel	The source/destination address is the manual configured IPv4 address	IPv6 address
Auto tunnel	IPv4 compatible IPv6 auto tunnel	The source address is the manual configured IPv4 address, and the destination address does not need to be	IPv4 compatible IPv6 address, its format: ::a.b.c.d/96
	6to4 tunnel		6to4 address, the format is:

Tunnel Type	Tunnel Mode	Tunnel Source/Destination Address	Tunnel Interface Address
		configured.	2002:a.b.c.d::/48
	ISATAP tunnel		ISATAP address, the format is: Prefix:0:5EFE:a.b.c.d/64

- IPv6 over IPv4 manual tunnel

This kind of tunnel is established manually. The terminal address of the tunnel is determined by the configuration. It is not necessary to assign special IPv6 addresses to the nodes. It is suitable for the IPv6 nodes that often communicate.

- IPv4 compatible with IPv6 auto tunnel

IPv4 compatible IPv6 auto tunnel is a point-to-multipoint tunnel. A special IPv6 address is used at both ends of the tunnel. Its format is: a.b.c.d/96, in which a.b.c.d is the IPv4 address. In the process of tunnel encapsulation, the embedded IPv4 address is automatically used as the end of the tunnel, which makes the establishment of the tunnel very convenient. However, due to the fact that the IPv4 compatible IPv6 address still depends on the IPv4 address in the application, this limitation can not be changed. Therefore, IETF has abandoned this kind of address in the new standard, and this kind of tunnel will be phased out.

- 6to4 tunnel

The 6to4 tunnel is a point-to-multipoint tunnel. Special IPv6 addresses are required at both ends of the tunnel in the format of 2002:a.b.c.d:/48, in which 2002 represents a fixed IPv6 address prefix and a.b.c.d represents the unique 32-bit IPv4 address corresponding to the 6to4 tunnel. This embedded IPv4 address is automatically used as the end point of the tunnel in the process of tunnel encapsulation, which makes the establishment of the tunnel very convenient. Therefore, the nodes using the 6to4 mechanism must have at least one unique IPv4 address in the world. This mechanism is suitable for the intercommunication between the nodes running IPv6. Since the first

48 bits in the IPv6 address prefix of 6to4 have been determined by the fixed number plus the IPv4 address, the remaining 16 bits subnet number can be defined by the user himself, which makes it more flexible to use the IPv4 network to realize the interconnection of the IPv6 network. 6to4 overcomes the limitation of IPv4 compatible IPv6 automatic tunnel.

- ISATAP tunnel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnels are point-to-multipoint automatic tunnels. Special IPv6 addresses are required at both ends of the tunnel in the format of Prefix: 0:5EFE: a.b.c.d/64, where Prefix represents any valid IPv6 unicast address prefix, and a.b.c.d represents 32-bit IPv4 address (not required to be globally unique). The embedded IPv4 address is automatically used as the end point of the tunnel during the tunnel encapsulation, so this kind of tunnel is also built automatically.

- Transition tunnel encapsulation

When IPv6 packets are sent through transitional tunnels, an IP header is added to the tunnel header, the protocol number in the IP header is 41, the source address in the IP header is set to the source address of the tunnel, and the destination address in the IP header is set according to the type of the tunnel: if it is a manual tunnel, it is set as the configured tunnel destination address, and if it is an automatic tunnel, it is set as the IPv4 address embedded in the IPv6 address.

- The structure of the transition tunnel packet

IPv4 Header	IPv6 Header	IPv6 Packet Payload

IPv6 Packet Payload: The payload of the IPv6 packet before entering the tunnel, which serves as the valid payload of the tunnel packet.

IPv6 Header: The header of the IPv6 packet before entering the tunnel.

IPv4 Header: The encapsulated outer IPv4 header, which is the transmission tool of the IPv6 packet across the IPv4 network.

- The forwarding of the transition tunnel packet

After the packet is encapsulated at the beginning of the transition tunnel, select the route according to the encapsulated destination address, and then, send the packet from the corresponding network interface. The intermediate device forwards it as an ordinary IP packet until the packet reaches the end of the tunnel.

- The encapsulation/de-capsulation of the transition tunnel packet

The de-capsulation process and the encapsulation process are opposite. The tunnel end first analyzes the IPv4 header after receiving the packet. If the destination address is its own address, check the protocol field of the IP header. If the protocol field is 41, hand over the packet to the transition tunnel for processing. After the tunnel removes the IPv4 header of the packet, select the route according to the destination address of the packet after de-capsulation, and perform the subsequent processing according to the result of the route selection.

5.9.2 Transition Tunnel Function Configuration

Table 500 Transition tunnel function configuration list

Configuration task	
Configure IPv6 over IPv4 manual tunnel	Configure IPv6 over IPv4 manual tunnel
Configure the IPv4 compatible IPv6 auto tunnel	Configure the IPv4 compatible IPv6 auto tunnel
Configure the 6to4 tunnel	Configure the 6to4 tunnel
Configure the ISATAP tunnel	Configure the ISATAP tunnel

Note

- For the configuration commands of the transition tunnel, refer to the chapter of IP Tunnel in the configuration manual.

5.9.2.1 Configure the IPv6 over IPv4 Manual Tunnel

Configuration Conditions

Before configuring the IPv6 over IPv4 manual tunnel, complete the following tasks:

- Configure the IP address of the physical interface, making the neighboring nodes reachable at the network layer
- Create one tunnel interface, and configure the basic parameters (refer to the configuration manual of the tunnel interface)
- Configure any unicast routing protocol, making the route at the two ends of the tunnel reachable

Configure IPv6 over IPv4 Manual Tunnel

Table 501 Configure IPv6 over IPv4 manual tunnel

Step		Command	Description
Enter the global configuration mode		configure terminal	-
Enter the tunnel configuration mode		interface tunnel *tunnel-number*	-
Configure the tunnel interface address	Configure IPv6 global unicast address or anycast address or the local address of the site or auto get address	ipv6 address { *ipv6-address/prefix-length* [anycast | eui-64] | autoconfig }	Mandatory By default, do not configure the IPv6 address on the tunnel interface.
	Configure the local address of the IPv6 link	ipv6 address *ipv6-address* link-local	Optional By default, after enabling the IPv6 on the interface, automatically generate the

Step	Command	Description
		local address of the link.
Configure the tunnel interface mode as the IPv6 over IPv4 manual tunnel	tunnel mode ipv6ip	Mandatory By default, the tunnel interface mode is GRE over IPv4.
Configure the source address or interface name of the tunnel interface	tunnel source { *ip-address* | *interface-name* }	Mandatory By default, do not configure the source address or interface name on the tunnel interface.
Configure the destination address or host name of the tunnel interface	tunnel destination { *ip-address* | *hostname* }	Mandatory By default, do not configure the destination address or host name on the tunnel interface.

Note

- The source address and destination address must be configured at both ends of the tunnel, and the addresses of the two ends are mutually the source address and destination address.
- If adopting the interface mode when configuring the tunnel source, the source address of the tunnel is the master address of the source interface.
- The two ends of the tunnel should be configured as the same tunnel mode. Otherwise, transmitting via the tunnel fails.
- On one device, you cannot configure multiple tunnels whose tunnel mode, source address, and destination address are all the same.

5.9.2.2 Configure IPv4 Compatible IPv6 Auto Tunnel

Configuration Conditions

Before configuring the IPv4 over IPv6 manual tunnel, complete the following tasks:

- Configure the IP address of the physical interface, making the neighboring nodes reachable at the network layer
- Create one tunnel interface, and configure the basic parameters (refer to the configuration manual of the tunnel interface)
- Configure any unicast routing protocol, making the route at the two ends of the tunnel reachable

Configure IPv4 Compatible IPv6 Auto Tunnel

Table 502 Configure IPv4 compatible IPv6 auto tunnel

Step		Command	Description
Enter the global configuration mode		configure terminal	-
Enter the tunnel configuration mode		interface tunnel *tunnel-number*	-
Configure the tunnel interface address	Configure IPv6 global unicast address or anycast address or the local address of the site or auto get address	ipv6 address { *ipv6-address/prefix-length* [anycast | eui-64] | autoconfig }	Mandatory By default, do not configure the IPv6 address on the tunnel interface.
	Configure the local address of the IPv6 link	ipv6 address *ipv6-address* link-local	Optional By default, after enabling the IPv6 on the interface, automatically generate the

Step	Command	Description
		local address of the link.
Configure the tunnel interface mode as the IPv4 compatible IPv6 auto tunnel	tunnel mode ipv6ip auto-tunnel	Mandatory By default, the mode of the tunnel interface is GRE over IPv4.
Configure the source address or interface name of the tunnel interface	tunnel source { *ip-address* | *interface-name* }	Mandatory By default, do not configure the source address and interface name on the tunnel interface.

Note

- IPv4 compatible IPv6 auto tunnel does not need to be configured with the destination address. When encapsulating the tunnel, the used destination address is the embeded IPv4 address auto got from IPv4 compatible IPv6 address.
- If adopting the interface mode when configuring the tunnel source, the source address of the tunnel is the master address of the source interface.
- The two ends of the tunnel should be configured as the same tunnel mode. Otherwise, transmitting via the tunnel fails.
- On one device, you can only configure one IPv4 compatible IPv6 auto tunnel.

5.9.2.3 Configure the 6to4 Tunnel

Configuration Conditions

Before configuring the 6to4 tunnel, complete the following tasks:

- Configure the IP address of the physical interface, making the neighboring nodes reachable at the network layer
- Create one tunnel interface, and configure the basic parameters (refer to the configuration manual of the tunnel interface)
- Configure any unicast routing protocol, making the route at the two ends of the tunnel reachable

Configure the 6to4 Tunnel

Table 503 Configure the 6to4 tunnel

Step		Command	Description
Enter the global configuration mode		configure terminal	-
Enter the tunnel configuration mode		interface tunnel *tunnel-number*	-
Configure the tunnel interface address	Configure IPv6 global unicast address or anycast address or the local address of the site or auto get address	ipv6 address { *ipv6-address/prefix-length* [anycast | eui-64] | autoconfig }	Mandatory By default, do not configure the IPv6 address on the tunnel interface.
	Configure the local address of the IPv6 link	ipv6 address *ipv6-address* link-local	Optional By default, after enabling IPv6 on the interface, automatically generate the local address of the link.
Configure the tunnel interface mode as 6to4 tunnel		tunnel mode ipv6ip 6to4	Mandatory By default, the tunnel interface mode is GRE over IPv4.

Step	Command	Description
Configure the source address or interface name of the tunnel interface	tunnel source { *ip-address* | *interface-name* }	Mandatory By default, do not configure the source address or interface name on the tunnel interface.

Note

- It is not necessary to configure the destination address for the 6to4 tunnel. The destination address used during tunnel encapsulation is automatically got from the imbedded IPv4 address in the 6to4 tunnel IPv6 address.
- If adopting the interface mode when configuring the tunnel source, the source address of the tunnel is the master address of the source interface.
- The two ends of the tunnel should be configured as the same tunnel mode. Otherwise, transmitting via the tunnel fails.
- On one device, you can only configure one 6to4 tunnel.

5.9.2.4 Configure the ISATAP Tunnel

Configuration Conditions

Before configuring the ISATAP tunnel, complete the following tasks:

- Configure the IP address of the physical interface, making the neighboring nodes reachable at the network layer
- Create one tunnel interface, and configure the basic parameters (refer to the configuration manual of the tunnel interface)
- Configure any unicast routing protocol, making the route at the two ends of the tunnel reachable

Configure the ISATAP Tunnel

Table 504 Configure the ISATAP tunnel

Step		Command	Description
Enter the global configuration mode		configure terminal	-
Enter the tunnel configuration mode		interface tunnel *tunnel-number*	-
Configure the tunnel interface address	Configure IPv6 global unicast address or anycast address or the local address of the site or auto get address	ipv6 address { *ipv6-address/prefix-length* [anycast | eui-64] | autoconfig }	Mandatory By default, do not configure the IPv6 address on the tunnel interface.
	Configure the local address of the IPv6 link	ipv6 address *ipv6-address* link-local	Optional By default, after enabling IPv6 on the interface, auto generate the local address of the link.
Configure the tunnel interface mode as the IPv4 compatible IPv6 auto tunnel		tunnel mode ipv6ip isatap	Mandatory By default, the tunnel interface mode is GRE over IPv4.
Configure the source address or interface name of the tunnel interface		tunnel source { *ip-address* | *interface-name* }	Mandatory By default, do not configure the source address or interface name on the tunnel interface.

Note

- It is not necessary to configure the destination address for the 6to4 tunnel. The destination address used during tunnel encapsulation is automatically got from the imbedded IPv4 address in the 6to4 tunnel IPv6 address.
- If adopting the interface mode when configuring the tunnel source, the source address of the tunnel is the master address of the source interface.
- The two ends of the tunnel should be configured as the same tunnel mode. Otherwise, transmitting via the tunnel fails.
- On one device, you cannot configure multiple ISATAP tunnels with the same source address at the same time.

5.9.2.5 Monitoring and Maintaining of Transition Tunnel

Table 505 Monitoring and maintaining of the transition tunnel

Command	Description
show tunnel [*tunnel-id*]	Displays the configuration information of all tunnels or a specified tunnel.

5.9.3 Typical Configuration Examples of Transition Tunnel

5.9.3.1 Configure Basic Functions of IPv6 over IPv4 Manual Tunnel

Network Requirements

- IPv6 Network1 and IPv6 Network2 are the private IPv6 network of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 communicate via the IPv6 over IPv4 manual tunnel between Device1 and Device3.

Network Topology

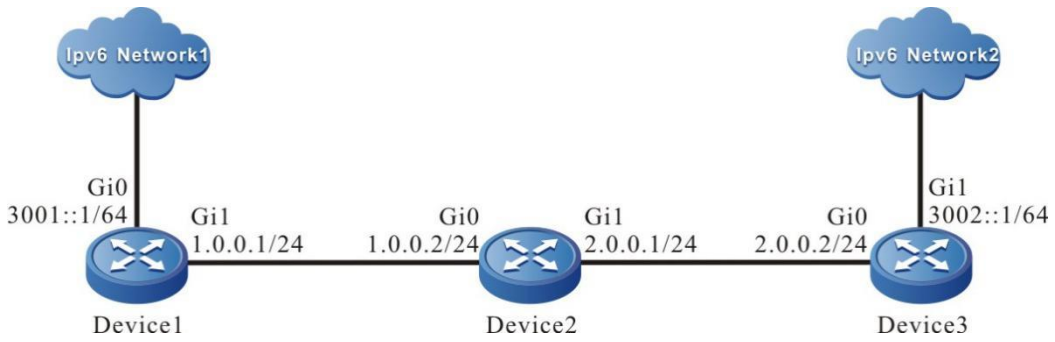


Figure 87 Networking for Configuring the basic functions of IPv6 over IPv4 manual tunnel

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF, making Device1, Device2, and Device3 communicate with each other.

#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)#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)#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)#exit
```

#Query the route 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 [110/65536] via 2.0.0.1, 00:18:40, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:22:27, gigabitethernet0
```

Note

- The querying methods of Device1 and Device2 are the same as that of Device3, so the querying process is omitted.

Step 3: Configure the IPv6 over IPv4 manual tunnel.

#On Device1, configure IPv6 over IPv4 manual tunnel tunnel1, the source address is 1.0.0.1, the destination address is 2.0.0.2, and the IPv6 address is 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#tunnel destination 2.0.0.2
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#On Device3, configure IPv6 over IPv4 manual tunnel tunnel1, the source address is 2.0.0.2, the destination address is 1.0.0.1, and the IPv6 address is 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ip
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#tunnel destination 1.0.0.1
Device3(config-if-tunnel1)#ipv6 address 10::2/64
Device3(config-if-tunnel1)#exit
```

#Query the IPv6 over IPv4 manual tunnel information of Device3.

```
Device3#show tunnel 1

Tunnel 1:
  Tunnel mode is ipv6ip
  Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface gigabitethernet0)
  Destination ipv4 address is 1.0.0.1
  Tunnel state is up
```

```
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Note

- The querying method of Device1is the same as that of Device3, so the querying process is omitted.
- When the tunnel is not in the same network segment, it is necessary to configure the static route to the peer tunnel on the devices at both ends of the tunnel, and the output interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to IPv6 Network2 with the egress interface tunnel1.

```
Device1(config)#ipv6 route 3002::/64 tunnel1
```

#On Device3, configure the static route to IPv6 Network1 with the egress interface tunnel1.

```
Device3(config)#ipv6 route 3001::/64 tunnel1
```

#Query the IPv6 route 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:20:35:50, lo0
C   10::/64 [0/0]
  via ::, 00:03:31, tunnel1
L   10::2/128 [0/0]
    via ::, 00:03:29, lo0
S   3001::/64 [1/100000]
  via ::, 00:00:01, tunnel1
```

```
C   3002::/64 [0/0]
  via ::, 00:00:06, gigabitethernet1
L   3002::1/128 [0/0]
    via ::, 00:00:04, lo0
```

Note

- The querying method of Device1 is the same as that of Device3, so the querying process is omitted.

5.9.3.2 Configure Basic Functions of IPv4 Compatible IPv6 Auto Tunnel

Network Requirements

- Device1 and Device2 have IPv4 and IPv6 dual protocol stack, and they communicate with each other through IPv4 network.
- An IPv4 compatible IPv6 automatic tunnel is established between Device1 and Device2, through which Device1 and Device2 communicate with each other.

Network Topology

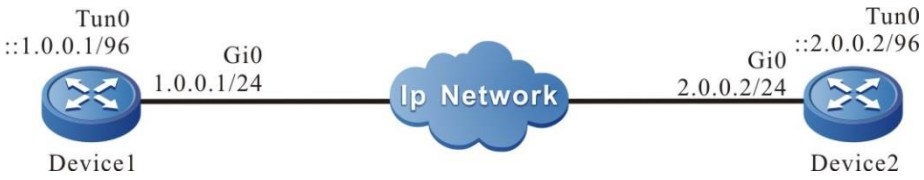


Figure 88 Networking of configuring the basic functions of IPv4 compatible IPv6 auto tunnel

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the IPv4 compatible IPv6 auto tunnel.

#On Device1, configure the IPv4 compatible IPv6 auto tunnel tunnel1, and the

source address is 1.0.0.1.

```
Device1#configure terminal
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip auto-tunnel
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#exit
```

#On Device2, configure IPv4 compatible IPv6 auto tunnel (tunnel1), and the source address is 2.0.0.2.

```
Device2#configure terminal
Device2(config)#interface tunnel 1
Device2(config-if-tunnel1)#tunnel mode ipv6ip auto-tunnel
Device2(config-if-tunnel1)#tunnel source 2.0.0.2
Device2(config-if-tunnel1)#exit
```

#View the interface information of Device2 tunnel1.

```
Device2#show ipv6 interface tunnel1
tunnel1 is up
  VRF: global
  IPv6 is enable, link-local address is fe80::0201:7aff:fe5e:d029
  Global unicast address(es):
::0200:0002, subnet is ::/96
  Joined group address(es):
    ff02::0001:ff00:0002
    ff02::0001:ff00:0
    ff02::0002
    ff02::0001
    ff02::0001:ff5e:d029
  ND control flags: 0x1
  MTU is 1480 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)
```

You can see that the interface of Device2 tunnel1 automatically generates IPv6 address::0200:0002.

Note

- IPv4 compatible IPv6 auto tunnel generates IPv4 compatible IPv6 address according to tunnel source address, and SOFINET devices display it in hexadecimal format.

#View the IPv6 route 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
C   ::/96 [0/0]
     via ::, 00:06:00, tunnel1
L   ::1/128 [0/0]
   via ::, 1w6d:20:35:50, lo0
L   ::200:2/128 [0/0]
     via ::, 00:05:59, lo0
```

#View the IPv4 compatible IPv6 auto tunnel information of Device2.

```
Device2#show tunnel 1
Tunnel 1:
   Tunnel mode is ipv6ip auto-tunnel
   Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface gigabitethernet0)
   Tunnel state is up
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Note

- The querying method of Device1 is the same as that of Device2, so the querying process is omitted.

Step 3: Check the result.

#On Device2, ping the IPv6 address of Device1 tunnel1 ::0100:0001.

```
Device2#ping ::0100:0001
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to ::100:1 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/3/16 ms.
```

#Device2 can ping the IPv6 address of Device1 tunnel1 :0100:0001.

5.9.3.3 Configure the Basic Functions of the 6to4 Tunnel

Network Requirements

- IPv6 Network1 and IPv6 Network2 are the private IPv6 network of Device1 and Device3 respectively.
- PC1 in IPv6 Network1 and PC2 in IPv6 Network2 communicate via the 6to4 tunnel between Device1 and Device3.

Network Topology

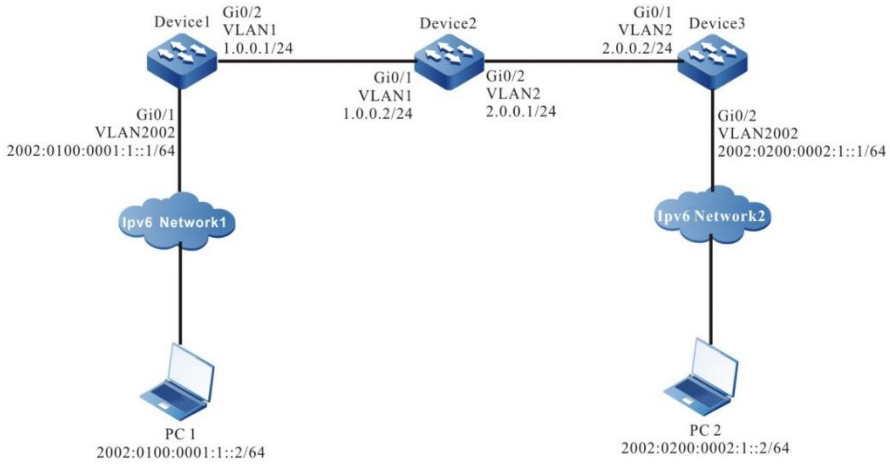


Figure 89 Networking for Configuring the basic functions of the 6to4 tunnel

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF, making Device1, Device2, and Device3 communicate with each other.

#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)#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)#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)#exit
```

#Query the route 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 [110/65536] via 2.0.0.1, 00:18:40, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:22:27, gigabitethernet0
```

Note

- The querying methods of Device1 and Device2 are the same as that of Device3, so the querying process is omitted.

Step 3: Configure the 6to4 tunnel.

#On Device1, configure the 6to4 tunnel (tunnel1), the source address is 1.0.0.1, and the IPv6 address is 2002:100:1::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
Device1(config-if-tunnel1)#ipv6 address 2002:100:1::1/64
```

```
Device1(config-if-tunnel1)#exit
```

#On Device3, configure the 6to4 tunnel (tunnel1), the source address is 2.0.0.2, and the IPv6 address is 2002:200:2::1.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#ipv6 address 2002:200:2::1/64
Device3(config-if-tunnel1)#exit
```

#Query the 6to4 tunnel information of Device3.

```
Device3#show iptl kernel
IP tunnel kernel information:
IP Tunnel Interface 1 (0x10001b3):
   Tunnel mode is ipv6ip 6to4
   Tunnel state is up
   Destination address is Unknown family
   Source address is 2.0.0.2
   Source interface is vlan2 (0x4000299)
   Time To Live (TTL) is 255
   Type Of Service (TOS) is not set
   VRF is global (0x0)
   Source interface VRF is global (0x0)
   Internal flags is 0x30000

total(1)
```

Note

- The querying method of Device1is the same as that of Device3, so the querying process is omitted.
- When the tunnel is not in the same network segment, it is necessary to configure the static routing to the peer tunnel on the devices at both ends of the tunnel, and the output interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to the segment 2002::/16 with the egress interface (tunnel1).

```
Device1(config)#ipv6 route 2002::/16 tunnel1
```

#On Device3, configure the static route to the segment 2002::/16 with the egress interface (tunnel1).

```
Device3(config)#ipv6 route 2002::/16 tunnel1
```

#Query the IPv6 route 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 ::, 6w1d:02:11:13, lo0
S   2002::/16 [1/100000]
    via ::, 00:10:31, tunnel1
C   2002:200:2::/64 [0/0]
    via ::, 00:12:51, tunnel1
L   2002:200:2::1/128 [0/0]
    via ::, 00:12:49, lo0
C   2002:200:2:1::/64 [0/0]
    via ::, 00:12:15, gigabitethernet1
L   2002:200:2:1::1/128 [0/0]
    via ::, 00:12:13, lo0
```

Note

- The querying method of Device1is the same as that of Device3, so the querying process is omitted.

Step 5: Check the result.

#On PC1, ping the PC2 address 2002:200:2:1::2.

```
C:\>ping6 2002:200:2:1::2 –s 2002:0100:0001:1::2

Pinging 2002:200:2:1::2 with 32 bytes of data:

Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms
Reply from 2002:200:2:1::2: time<1ms

Ping statistics for 2002:200:2:1::2:
```

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

#PC1 can ping PC2 address 2002:200:2:1::2.

5.9.3.4 Configure 6to4 Tunnel Relay

Network Requirements

- Device1 is 6to4 relay device.
- IPv6 Network1 and IPv6 Network2 are the private IPv6 network of Device1 and Device3 respectively.
- PC1 in IPv6 Network1 and PC2 in IPv6 Network2 communicate via the 6to4 tunnel between Device1 and Device3.

Network Topology

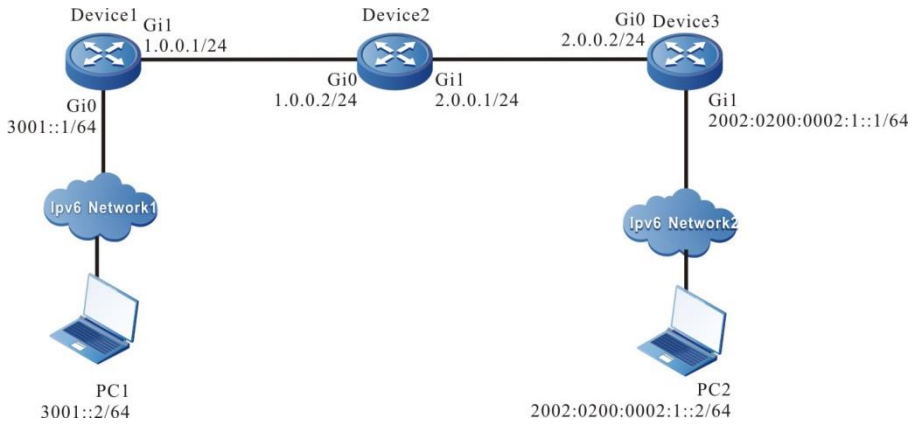


Figure 90 Networking of configuring the 6to4 tunnel relay

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPF, making Device1, Device2, and Device3 communicate with each other.

#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)#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)#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)#exit
```

#View the route 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 [110/65536] via 2.0.0.1, 00:18:40, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:22:27, gigabitethernet0
```

Note

- The querying methods of Device1 and Device2 are the same as that of Device3, so the querying process is omitted.

Step 3: Configure the 6to4 tunnel.

#On Device1, configure the 6to4 tunnel (tunnel1), the source address is 1.0.0.1, and IPv6 address is 2002:100:1::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device1(config-if-tunnel1)#tunnel source 1.0.0.1
```

```
Device1(config-if-tunnel1)#ipv6 address 2002:100:1::1/64
Device1(config-if-tunnel1)#exit
```

#On Device3, configure the 6to4 tunnel (tunnel1), the source address is 2.0.0.2, and IPv6 address is 2002:200:2::1.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6ip 6to4
Device3(config-if-tunnel1)#tunnel source 2.0.0.2
Device3(config-if-tunnel1)#ipv6 address 2002:200:2::1/64
Device3(config-if-tunnel1)#exit
#View the 6to4 tunnel information of Device3.
Device3#show tunnel 1
Tunnel 1:
  Tunnel mode is ipv6ip 6to4
  Source ipv4 address is 2.0.0.2(Source ipv4 address is up on source interface gigabitethernet0)
  Tunnel state is up
  Encapsulation vrf is global(0x0)
  TTL(time-to-live) is 255
  TOS(type of service) is not set
total(1)
```

Note

- The viewing method of Device1 is the same as that of Device3, and the viewing process is omitted.
- When the tunnel is not in the same network segment, the static route to the peer end tunnel needs to be configured on the devices at both ends of the tunnel, and the egress interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to the egress interface tunnel1 of the segment 2002::/16.

```
Device1(config)#IPv6 route 2002::/16 tunnel1
```

#On Device3, configure the static route to the egress interface tunnel1 of the segment 2002::/16, and configure the static route to the gateway 2002:100:1::1 of the

segment 3001::/64.

```
Device3(config)#IPv6 route 2002::/16 tunnel1
Device3(config)#IPv6 route 3001::/64 2002:100:1::1
```

#View the Ipv6 route 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 ::, 6w1d:02:11:13, lo0
S   2002::/16 [1/100000]
     via ::, 00:10:31, tunnel1
C   2002:200:2::/64 [0/0]
     via ::, 00:12:51, tunnel1
L   2002:200:2::1/128 [0/0]
     via ::, 00:12:49, lo0
C   2002:200:2:1::/64 [0/0]
     via ::, 00:12:15, gigabitethernet1
L   2002:200:2:1::1/128 [0/0]
     via ::, 00:12:13, lo0
S   3001::/64 [1/100000]
     via 2002:100:1::1, 00:00:53, tunnel1
```

Note

- The querying method of Device1 is the same as that of Device3, so the querying process is omitted.

Step 4: Configure the static route.

#On PC2, ping the address of PC1 3001::2.

```
C:\>ping6 3001::2 –s 2002:0200:0002:1::2

Pinging 3001::2 with 32 bytes of data:

Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
Reply from 3001::2: time<1ms
```

```
Ping statistics for 3001::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#PC2 can ping the address 3001::2 of PC1.

5.9.3.5 Configure Basic Functions of ISATAP Tunnel

Network Requirements

- Device and PC2 communicate with each other via the IPv4 network.
- PC2 is the ISATAP host, setting up the ISATAP tunnel with Device.
- PC1 in IPv6 Network and PC2 in IP Network perform the IPv6 communication via the ISATAP tunnel.

Network Topology

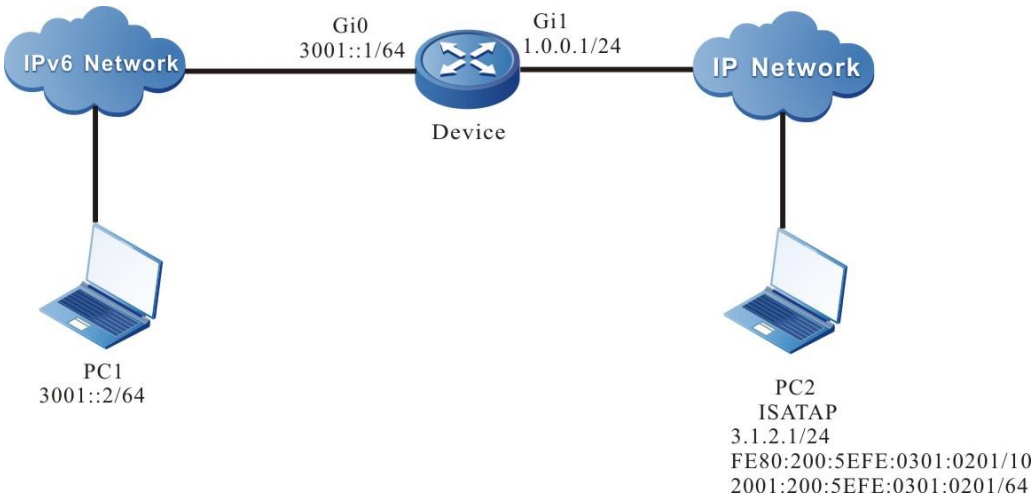


Figure 91 Networking for Configuring the basic functions of the ISATAP tunnel

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: On Device, configure the ISATAP tunnel.

#On Device, configure the ISATAP tunnel (tunnel1), the source address is 1.0.0.1, and the IPv6 address is 2001::5efe:100:1.

```
Device#configure terminal
Device(config)#interface tunnel 1
Device(config-if-tunnel1)#tunnel mode ipv6ip isatap
Device(config-if-tunnel1)#tunnel source 1.0.0.1
Device(config-if-tunnel1)#ipv6 address 2001::5efe:100:1/64
Device(config-if-tunnel1)#exit
```

#Query the IPv6 route table of Device.

```
Device#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 ::, 6d:05:16:46, lo0
C   2001::/64 [0/0]
     via ::, 00:07:56, tunnel1
L   2001::5efe:100:1/128 [0/0]
     via ::, 00:07:54, lo0
C   3001::/64 [0/0]
     via ::, 02:42:37, gigabitethernet0
L   3001::1/128 [0/0]
     via ::, 02:42:36, lo0
```

#Query the ISATAP tunnel information of Device.

```
Device#show tunnel 1


Tunnel 1:
   Tunnel mode is ipv6ip isatap
   Source ipv4 address is 1.0.0.1(Source ipv4 address is up on source interface gigabitethernet1)
   Tunnel state is up
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Step 3: On Device, disable the RA response suppression function of Tunnel1.

#On Device, disable the RA response suppression function of Tunnel1.

```
Device(config)#interface tunnel 1
Device(config-if-tunnel1)#no ipv6 nd suppress-ra response
Device(config-if-tunnel1)#exit
```

Step 4: Configure the ISATAP host PC2.

#On the host, the configuration of the ISATAP tunnel varies with the operation system. This text takes the Windows 10 operation system as an example to describe.

#Press WIN+R to open operation, input services.msc and press **Enter**.

#In the pop-up page, find IP Helper, right-click and select **Start**.

#Press WIN+R to open operation, enter cmd and press **Enter**.

#In the pop-up cmd window, enable the ISATAP tunnel function.

```
C:\Windows\system32>netsh interface ipv6 isatap set state enabled
Ok.
```

#Enter the ipconfig command in the cmd window of PC2 to view the ISATAP interface.

```
Tunnel adapter isatap.{AA8D619F-C31A-4255-8AA0-F43DF53EB61C}:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::200:5efe:3.1.2.1%38
   Default Gateway . . . . . . . . . :
```

PC2 automatically generates the link local address fe80:: 200:5efe: 3.1.2.1 in ISATAP format, and does not get the address prefix.

#Configure the destination address of ISATAP tunnel in cmd window of PC2 as 1.0.0.1.

```
C:\Windows\system32>netsh interface ipv6 isatap set router 1.0.0.1
Ok.
```

#Normally, input the ipconfig command in the cmd window to view the information of the ISATAP interface.

```
Tunnel adapter isatap.{AA8D619F-C31A-4255-8AA0-F43DF53EB61C}:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001::200:5efe:3.1.2.1
   Link-local IPv6 Address . . . . . : fe80::200:5efe:3.1.2.1%38
```

```
Default Gateway . . . . . : fe80::5efe:1.0.0.1%38
```

The ISATAP interface of PC2 gets the address prefix 2001::/64, and generates the global unicast address 2001::200:5efe:3.1.2.1.

Step 5: Check the result.

#On PC1, ping the address of PC2 ISATAP interface 2001::200:5efe:3.1.2.1.

```
C:\Windows\system32>ping 2001::200:5efe:3.1.2.1

Pinging 2001::200:5efe:3.1.2.1 with 32 bytes of data:
Reply from 2001::200:5efe:3.1.2.1: time<1ms
Reply from 2001::200:5efe:3.1.2.1: time<1ms
Reply from 2001::200:5efe:3.1.2.1 :time<1ms
Reply from 2001::200:5efe:3.1.2.1: time<1ms

Ping statistics for 2001::200:5efe:3.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#PC1 can ping the address of PC2 IPv6 interface2 2001::200:5efe:3.1.2.1.

5.10 IPv6 Tunnel

5.10.1 Overview

IPv6 tunnel (Generic Packet Tunneling in IPv6) is one of tunnel technologies. The starting and ending points of the tunnel need to be manually configured. It is a virtual point-to-point connection. It provides a transmission channel for encapsulated packets. The two ends of the tunnel encapsulate and de-capsulate the packet respectively. The IPv6 tunnel can encapsulate IPv4 and IPv6 packets, so that these encapsulated packets can be transmitted in another IPv6 network.

- IPv6 tunnel encapsulation

When the IPv4 or IPv6 packets are sent through the IPv6 tunnel, an IPv6 packet header is added to the header, the Next Header field in the IPv6 packet header is set to 4 or 41, the source address in the IPv6 packet header is set to the source address of the tunnel, and the destination address in the IPv6 packet header is set as the destination

address of the tunnel.

- The structure of the IPv6 tunnel packet

IPv6 Header	Original Header	Original Packet Payload

Original Packet Payload: The payload of the packet before entering the tunnel, which serves as the valid payload of the tunnel packet.

Original Header: The header of the packet before entering the tunnel, such as IPv4 or IPv6 header

IPv6 Header: The encapsulated outer IPv6 packet header, which is the transmission tool of the original packet across the IPv6 network.

- The forwarding of the IPv6 tunnel packet

After the packet is encapsulated at the beginning of the IPv6 tunnel, select the route according to the encapsulated destination address, and then, send the packet from the corresponding network interface. The intermediate device forwards it as an ordinary IPv6 packet until the packet reaches the end of the tunnel.

- The encapsulation/de-capsulation of the IPv6 tunnel packet

The de-capsulation process and the encapsulation process are opposite. The tunnel end first analyzes the IPv6 header after receiving the packet. If the destination address is its own address, check the Next Header field of the IPv6 header. If the Next Header field is 4 or 41, hand over the packet to the IPv6 tunnel for processing. After the tunnel removes the IPv6 header of the packet, select the route according to the packet type and destination address of the packet after de-capsulation, and perform the subsequent processing according to the result of the route selection.

5.10.2 IPv6 Tunnel Function Configuration

Table 506 IPv6 tunnel function configuration list

Configuration task	
Configure the IPv6 tunnel	Configure the IPv6 tunnel

5.10.2.1 Configure an IPv6 Tunnel

Configuration Conditions

Before configuring the IPv6 tunnel, complete the following tasks:

- Configure the IPv6 address of the physical interface, making the neighboring nodes reachable at the network layer.
- Create one tunnel interface, and configure the basic parameters (refer to the configuration manual of the tunnel interface).
- Configure any unicast routing protocol, making the route at the two ends of the tunnel reachable.

Configure an IPv6 Tunnel

Table 507 Configure an IPv6 tunnel

Step		Command	Description
Enter the global configuration mode		configure terminal	-
Enter the tunnel configuration mode		interface tunnel *tunnel-number*	-
Configure the tunnel interface address	Configure the IPv4 unicast address	ip address *ip-address* { *mask* | *mask-length* }	Either By default, do not configure the address on the tunnel interface.
	Configure IPv6 global unicast address or anycast address or the local address of the site or auto get address	ipv6 address { *ipv6-address/prefix-length* [anycast | eui-64] | autoconfig }	
	Configure the local address of the IPv6 link	ipv6 address *ipv6-address* link-local	Optional By default, after the interface enables IPv6, automatically generate the local address of the

Step	Command	Description
		link.
Configure the tunnel interface mode as the IPv6 tunnel	tunnel mode ipv6	Mandatory By default, the tunnel interface mode is GRE over IPv4.
Configure the source address or interface of the tunnel interface	tunnel source { *ipv6-address* | *interface-name* }	Mandatory By default, do not configure the source address or interface name on the tunnel interface.
Configure the destination address or host name of the tunnel interface	tunnel destination { *ipv6-address* | *hostname* }	Mandatory By default, do not configure the destination address or host name on the tunnel interface.

Note

- The source address and destination address must be configured at both ends of the tunnel, and the addresses of the two ends are mutually the source address and destination address.
- If adopting the interface mode when configuring the tunnel source, the source address of the tunnel is the IPv6 address of the source interface.
- The two ends of the tunnel should be configured as the same tunnel mode. Otherwise, transmitting via the tunnel fails.
- On one device, you cannot configure multiple tunnels whose tunnel mode, source address, and destination address are all the same.

5.10.2.2 IPv6 Tunnel Monitoring and Maintaining

Table 508 IPv6 tunnel monitoring and maintaining

Command	Description
show tunnel [*tunnel-id*]	Display the configuration information of all tunnels or the specified tunnel

5.10.3 Typical Configuration Example of IPv6 Tunnel

5.10.3.1 Configure Basic Functions of IPv6 Tunnel

Network Requirements

- IP Network1 and IP Network2 are the private IP network of Device1 and Device3 respectively.
- IPv6 Network1 and IPv6 Network2 communicate via the IPv6 over IPv4 manual tunnel between Device1 and Device3.
- IP Network1 and IP Network2 communicate via the IPv6 tunnel between Device1 and Device3.
- IPv6 Network1 and IPv6 Network2 communicate via the IPv6 tunnel between Device1 and Device3.

Network Topology

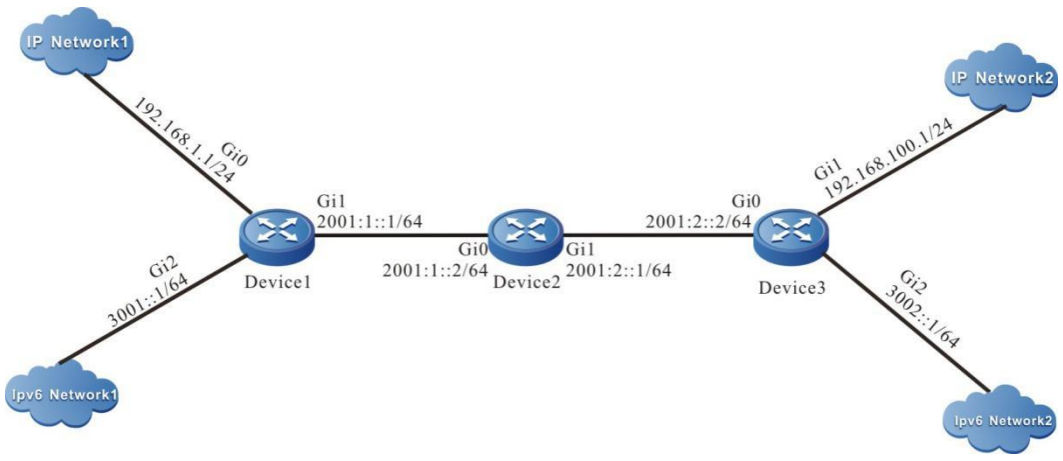


Figure 92 Networking for Configuring the basic functions of the IPv6 tunnel

Configuration Steps

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure OSPFv3, making Device, Device2, and Device3 communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.75.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ipv6 router ospf tag 100 area 0
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 1.2.75.1
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 router ospf tag 100 area 0
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ipv6 router ospf tag 100 area 0
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 1.1.73.1
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ipv6 router ospf tag 100 area 0
Device3(config-if-gigabitethernet0)#exit
```

#Query the IPv6 route 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 ::, 6w0d:23:09:31, lo0
O   2001:1::/64 [110/2]
    via fe80::508b:fff:fee4:ff6, 00:08:37, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 00:15:51, gigabitethernet0
L   2001:2::2/128 [0/0]
    via ::, 00:15:50, lo0
C   3002::/64 [0/0]
    via ::, 00:15:06, gigabitethernet2
L   3002::1/128 [0/0]
    via ::, 00:15:04, lo0
```

Note

- The querying methods of Device1 and Device2 are the same as that of Device3, so the querying process is omitted.

Step 3: Configure the IPv6 tunnel.

#On Device1, configure the IPv6 tunnel (tunnel1), the source address is 2001:1::1, destination address is 2001:2::2, IP address is 10.0.0.1, and IPv6 address is 10::1.

```
Device1(config)#interface tunnel 1
Device1(config-if-tunnel1)#tunnel mode ipv6
Device1(config-if-tunnel1)#tunnel source 2001:1::1
Device1(config-if-tunnel1)#tunnel destination 2001:2::2
Device1(config-if-tunnel1)#ip address 10.0.0.1 255.255.255.0
Device1(config-if-tunnel1)#ipv6 address 10::1/64
Device1(config-if-tunnel1)#exit
```

#On Device3, configure the IPv6 tunnel (tunnel1), the source address is 2001:2::2, destination address is 2001:1::1, IP address is 10.0.0.2, and IPv6 address is 10::2.

```
Device3(config)#interface tunnel 1
Device3(config-if-tunnel1)#tunnel mode ipv6
Device3(config-if-tunnel1)#tunnel source 2001:2::2
Device3(config-if-tunnel1)#tunnel destination 2001:1::1
Device3(config-if-tunnel1)#ip address 10.0.0.2 255.255.255.0
Device3(config-if-tunnel1)#ipv6 address 10::2/64
```

```
Device3(config-if-tunnel1)#exit
#Query the IPv6 tunnel information of Device3.
Device3#show tunnel 1

Tunnel 1:
   Tunnel mode is ipv6
      Gre checksum validation is disabled
      Gre key is not set
   Source ipv6 address is 2001:2::2 (Source ipv6 address is up on source interface gigabitethernet0)
   Destination ipv6 address is 2001:1::1
   Tunnel state is up
   Encapsulation vrf is global(0x0)
   TTL(time-to-live) is 255
   TOS(type of service) is not set
total(1)
```

Note

- The querying method of Device1 is the same as that of Device3, so the querying process is omitted.
- When the tunnel is not in the same network segment, it is necessary to configure the static route to the peer tunnel on the devices at both ends of the tunnel, and the output interface is the tunnel interface.

Step 4: Configure the static route.

#On Device1, configure the static route to IP Network2 with the egress interface tunnel1.

```
Device1(config)#ip route 192.168.100.0 255.255.255.0 tunnel1
```

#On Device1, configure the static route to IPv6 Network2 with the egress interface tunnel1.

```
Device1(config)#ipv6 route 3002::/64  tunnel1
```

#On Device3, configure the static route to IP Network1 with the egress interface tunnel1.

```
Device3(config)#ip route 192.168.1.0 255.255.255.0 tunnel1
```

#On Device3, configure the static route to IPv6 Network1 with the egress interface tunnel1.

```
Device3(config)# ipv6 route 3001::/64  tunnel1
```

#Query the route 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   10.0.0.0/24 is directly connected, 00:17:12, tunnel1
S   192.168.1.0/24 [1/100000] is directly connected, 00:00:10, tunnel1
C   192.168.100.0/24 is directly connected, 00:00:28, gigabitethernet1
#Query the IPv6 route 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 ::, 6w0d:23:50:28, lo0
C   10::/64 [0/0]
    via ::, 00:12:23, tunnel1
L   10::2/128 [0/0]
    via ::, 00:12:22, lo0
O   2001:1::/64 [110/2]
    via fe80::508b:fff:fee4:ff6, 00:49:34, gigabitethernet0
C   2001:2::/64 [0/0]
    via ::, 00:56:48, gigabitethernet0
L   2001:2::2/128 [0/0]
    via ::, 00:56:46, lo0
S   3001::/64 [1/100000]
    via ::, 00:00:14, tunnel1
C   3002::/64 [0/0]
    via ::, 00:56:02, gigabitethernet2
L   3002::1/128 [0/0]
    via ::, 00:56:01, lo0
```

Note

- The querying method of Device1 is the same as that of Device3, so the querying process is omitted.

6 Unicast Routing

6.1 Routing Basics

6.1.1 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 routing 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.

6.1.2 Routing Basic Function Configuration

Table 509 Routing Basic Function List

Configuration Tasks	
Configure load balancing for routing.	Configure the maximum number of load balancing entries.
	Configure the calculation mode of the load balancing
Configure VRF route capacity	Configure VRF route capacity

6.1.2.1 Configure Load Balancing for Routing

Configuration Condition

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 510 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 64.

Configure Calculation Mode of Load Balancing

There are three calculation methods for load balancing:

- Calculation method based on source address and destination address: Identify a flow with source address and destination address, and the packets of the same flow take the same path without disorder. When the load of each flow is unbalanced, the line load may be unbalanced.
- Calculation method based on source address: Only source address is used to identify a flow. The packets of the same flow use the same path to ensure that the same flow takes the same path and will not be out of order. When the load of each stream is unbalanced, the line load may be unbalanced.
- Packet-based calculation method: The packets to the same destination take different paths to achieve load balance on each path as much as possible, but may be out of order.

Table 511 Configure the calculation mode of the load balancing

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the load balancing mode of the IPv4 packet	ip load-sharing { per-destination | per-packet | per-source }	Optional By default, use the calculation mode based on source and destination addresses.

6.1.2.2 Configure VRF Route Capacity

Configuration Condition

None

Configure VRF Route Capacity

In order to ensure the normal use of devices and prevent excessive resources consumed by a large number of routes, users can configure **routing-table limit** to limit

the capacity of routes under each VRF, and generate alarm information when the routing volume reaches the set value.

Table 512 Configure the VRF route capacity

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the VRF configuration mode	ip vrf *vrf-name*	-
Configure the VRF route capacity	routing-table limit *limit-value* { *threshold-value* | syslog-alert }	Optional By default, the route capacity is 880000. When the routes reach the 80% of the route capacity, print the alarm information.

Note

- This command cannot limit the route capacity in global VRF.
- If the route items exceed the capacity, the new route information will be lost.

6.1.2.3 Routing Basics Monitoring and Maintaining

Table 513 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-*	Display IP route information.

Command	Description
address { *mask* | *mask-len* }]	

6.2 IPv6 Routing Basics

6.2.1 Overview

After a device receives an IPv6 packet through an interface, the device selects a route according to the destination address 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 address of the packet. 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 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 routing policy. A routing protocol that is used within an autonomous domain is an IGP. Common IGPs include RIPng, 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.

6.2.2 IPv6 Routing Basis Function Configuration

Table 514 IPv6 routing basis function configuration list

Configuration Task	
Configure the IPv6 route load balance	Configure the IPv6 load balance calculation mode

6.2.2.1 Configure Load Balancing of IPv6 Route

Configuration Condition

None

Configure the Calculation Mode of IPv6 Load Balance

The load balance has the following three kinds of calculation modes:

- Calculation mode based on source and destination addresses: Identify a flow with the source address and destination address. The packets of the same stream use the same path and is not disorderly. When the loads of the flows are unbalanced, it may lead to unbalanced line load.
- Calculation based on source address: Only the source address is used to identify a flow. The packets of the same flow use the same path to ensure that the same flow follows the same path without disorder. When the loads of the flows is unbalanced, it may lead to unbalanced line load.
- Calculation based on packets: The packets to the same destination adopt different paths to achieve load balancing on each path as far as possible, but may be disorderly.

Table 515 Configure the IPv6 load balancing calculation mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Configure the load balancing mode of the IPv6 packet	ipv6 load-sharing { per-destination | per-packet | per-source }	Optional By default, use the calculation mode based on the source and destination addresses.

6.2.2.2 Monitoring and Maintaining of IPv6 Route Basis

Table 516 Monitoring and maintaining of the IPv6 route basis

Command	Description
clear ipv6 route { *ipv6-address* | *ipv6-prefix* | all }	Clear the specified IPv6 route in the route table
show ipv6 route [vrf *vrf-name*] [*ipv6-address* | *ipv6-prefix* | bgp | brief | connected | isis | linklocal | local | ospf | rip | static | statistic | all]	Display the IPv6 route information

6.3 Static Routes

6.3.1 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.

Null0 is a special route, with the route output interface as the Null0 interface. The Null0 interface is always in the UP status but it cannot forward packets. The packets that are sent to the interface will be discarded. If you configure a static route and specify the output interface for a certain network segment to Null0, the packets that are sent to the network segment will be discarded. Therefore, you can configure realize packet filtration by configuring Null0 static routes.

6.3.2 Static Routing Function Configuration

Table 517 Static Route Configuration Function List

Configuration Tasks	
Configure a static route.	Configure a static route.

Configuration Tasks	
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.
Configure a floating route.	Configure a floating route.
Configure a static route to coordinate with BFD.	Configure a static route to coordinate with BFD.
Configure a static route to coordinate with Track.	Configure a static route to coordinate with Track.

6.3.2.1 Configure a Static Route

Configuration Condition

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 518 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-	Mandatory. The field *administrative-distance* is the administrative distance of the static route. If

Step	Command	Description
	name] [tag tag-value] [track track-id] [arp-detect-lookup] [administrative-distance]	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.

6.3.2.2 Configure the Default Administrative Distance

Configuration Condition

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 519 Configuring the Default Administrative Distance

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

Step	Command	Description
Enters the static route configuration mode.	router static	-
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.

6.3.2.3 Configure the Recursive Function

Configuration Condition

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 520 Configure the Recursive Function

Step	Command	Description
Enter the global	configure terminal	-

Step	Command	Description
configuration mode.		
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.

6.3.2.4 Configure Load Balancing Routes

Configuration Condition

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 521 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	ip route *destination-ip-address*	Mandatory.

Step	Command	Description
balancing route.	*destination-mask interface-name2 distance*	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.

6.3.2.5 Configure a Floating Route

Configuration Condition

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 522 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*	Mandatory. The output interface of the

Step	Command	Description
	distance1	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.

6.3.2.6 Configure Static Route to Coordinate with BFD

Configuration Condition

None

Configure a Static Route to Coordinate with BFD

The Bidirectional Forwarding Detection (BFD) protocol provides a method for detecting the connectivity of the forwarding path between two adjacent routers with light load. A protocol neighbor can quickly detect the connectivity fault of a forwarding path. Different from other dynamic protocol routes, static routes cannot learn communication link failures. BFD provides a method for quickly detecting communication link failures for static routes. After a static route is configured to

coordinate with BFD, fast switchover of routes can be implemented. Currently, a static route only supports the asynchronous BFD detection mode. Therefore, you need to configure the route to coordinate with BFD on the devices at the two end of the link.

If the status of BFD that is coordinated with the static route is DOWN, the static route becomes invalid.

Table 523 Configuring an IPv4 static route to coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure a static route.	ip route *destination-ip-address destination-mask interface-name nexthop-ip-address*	Mandatory. Only the static route with both output interface and gateway address specified can coordinate with BFD.
Configure the output interface and the next-hop address for the route that is coordinated with BFD.	ip route static bfd *interface-name nexthop-ip-address*	Mandatory. The field *nexthop-ip-address* specifies the directly connected next-hop address.

Note

- For introduction of BFD and how to configure its basic functions, refer to BFD configuration manual.

6.3.2.7 Configure a Static Route to Coordinate with Track

Configuration Condition

None

Configure a Static Route to Coordinate 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 524 Configuring a Static Route to Coordinate 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	-

Step	Command	Description
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.

6.3.2.8 Configure Fast Re-routing of Static Route

Configuration Condition

Before configuring the fast re-routing of the static route, first complete the following task:

Use the route map to specify the egress interface and next hop of the standby route

Configure Fast Re-routing of Static Route

In the network using the static route, the traffic interruption caused by the link or device fault will continue until the protocol detects the link fault and the floating route takes effect. Usually, the traffic interruption lasts several seconds. To reduce the taffic interruption time, you can configure the fast re-routing of the static route. Set the backup next hop for the matched route by applying the route map. Once the master link fails, the traffic over the master link switches to the standby link at once, realizing the fast switching.

Table 525 Configure the fast re-routing of the static route

Step	Command	Description
Enter the system configuration mode	configure terminal	-
Configure the fast re-	ip route static fast-reroute	Mandatory

Step	Command	Description
routing of the static route	route-map *map-name*	By default, do not enable the fast re-routing.
Configure the auto fast re-routing of the static route	ip route static pic	Mandatory By default, do not enable the auto fast re-routing.

Note

- Only the static route specified with the egress interface and gateway address can perform the fast re-routing.
- When the fast re-routing based on route-map **set fast-reroute backup-nexthop** is auto, the protocol performs the auto fast re-routing.
- When using pic mode, the protocol performs the auto fast re-routing.
- The modes of enabling the fast re-routing are mutually exclusive.

6.3.2.9 Static Route Monitoring and Maintaining

Table 526 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.

6.3.3 Typical Configuration Example of Static Routes

6.3.3.1 Configure Static Routing Basic Functions

Network Requirement

- On Device1, Device2 and Device3, configure static routes so that PC1 and PC2 can communicate with each other.

Network Topology

Figure 93 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
```

```
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
        U - Per-user Static route
        O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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.

6.3.3.2 Configure a Floating Static Route

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

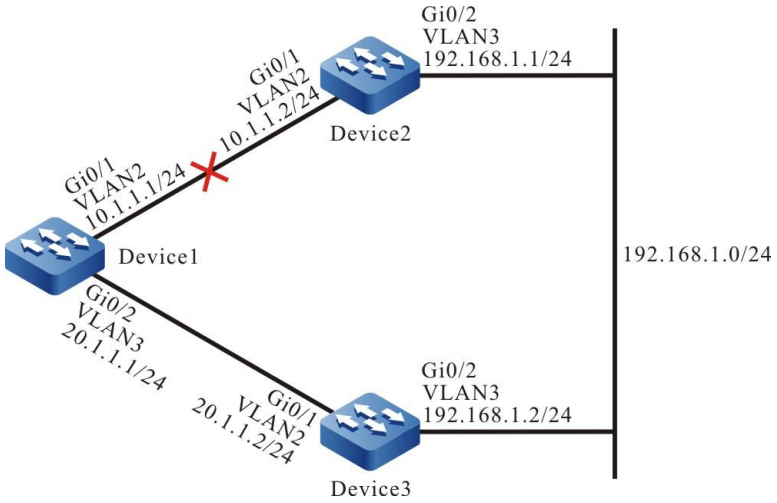


Figure 94 Networking for Configure a Floating Static Route

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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.

6.3.3.3 Configure a Static Route with the Null0 Interface

Network Requirements

- On Device1 and Device2, configure a default static route respectively, and configure the gateway addresses to the peer interface addresses of the two devices. On Device1, configure a static with the Null0 interface to filter only data that is sent to PC2.

Network Topology

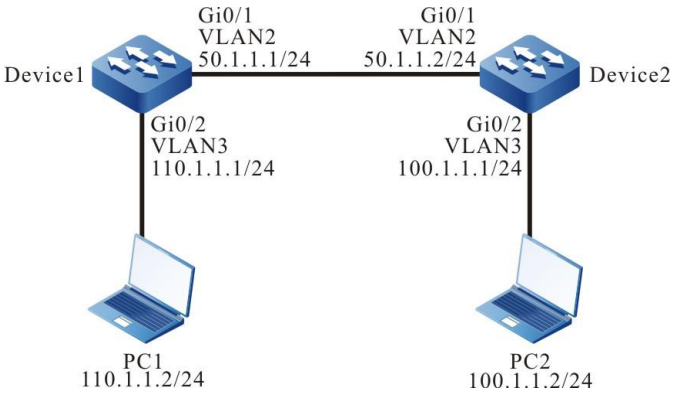


Figure 95 Networking for Configuring a Static Route with the Null0 Interface

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 static routes.

#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 check the connectivity with 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 route with the Null0 interface.

#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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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
```

In the routing table, the static route with the Null0 interface has been added.

#On PC1, use the **ping** command to check the connectivity with 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)
```

The ICMP packets sent by PC1 are found to be targeted at interface Null0 according to the routing table in Device1; therefore, the packets are discarded. In this way, PC1 fails to communicate with PC2.

Note

- A static route with the Null0 interface is a special route. The packets sent to the Null0 interface will be discarded. Therefore, configuring a route with the Null0 interface implements packet filtration.

6.3.3.4 Configure a Static Recursive Route

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

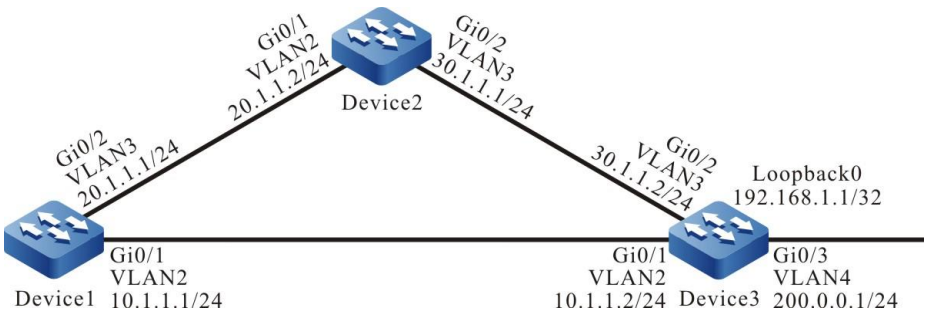


Figure 96 Networking for Configure a Static Recursive Static Route

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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.

6.3.3.5 Configure Static Route to Coordinate with BFD

Network Requirements

- On Device1, configure two static routes to network segment 201.0.0.0/24. One route passes Device2 while the other route passes Route3. Device first uses the route that passes Device 3 to forward packets. Similarly, on Device3, configure two static routes to network segment 200.0.0.0/24. Device3 first uses the route that passes Device1 to forward packets.
- On Device1 and Device3, configure static routes to coordinate with BFD. When the route between Device1 and Device3 is faulty, they can quickly switch over to the route that passes Device2.

Network Topology

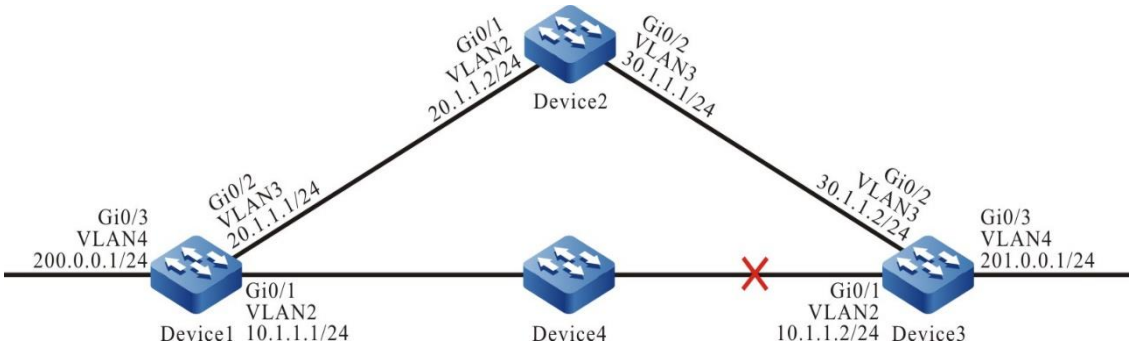


Figure 97 Networking for configuring a static route to coordinate with BFD

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure static routes.

#On Device1, configure two static routes to 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
```

#On Device2, configure two static routes to 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
```

#On Device3, configure two static routes to 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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external

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 coordinate 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 4: 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 BFD sessions have been normally set up on Device1 and Device3, indicating that the static routes are configured to coordinate with BFD successfully.

#When the route between Device1 and Device3 is faulty, BFD quickly detects the line fault and switch over to the route that passes Device2 for communication. Query the BFD session and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
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 handling method on Device3 is the same as that on Device1.

6.3.3.6 Configure Fast Re-routing of Static Route

Network Requirements

- Device1 configures two static routes to the network 192.168.1.1/32. One is reachable via Device2 and the other is reachable via Device3. Device1 first uses the line with Device3 to forward the packet. Similarly, Device3 configures two static routes to the network 100.1.1.1/32. Device3 first uses the line with Device1 to forward the packet.
- Device1 and Device3 enable the fast re-routing of the static route. When the line between Device1 and Device3 fails, the service can switch to Device2 for communication fast.

Network Topology

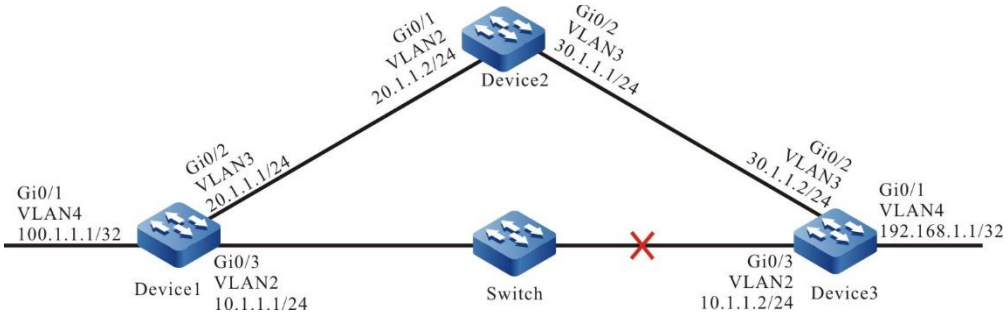


Figure 98 Configure the fast re-routing of the static route

Configuration Steps

Step 1: Configure the IP addresses of the interfaces. (Omitted)

Step 2: Configure static routes.

#Configure Device1: configure two static routes to the network 192.168.1.1/32. The management distance of the route with the gateway 20.1.1.2 is 10, making it become the floating route.

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.1 255.255.255.255 vlan 2 10.1.1.2
Device1(config)#ip route 192.168.1.1 255.255.255.255 vlan 3 20.1.1.2 10
```

#Configure Device2: configure the static route to the network 100.1.1.1/32 and 192.168.1.1/32.

```
Device2#configure terminal
Device2(config)#ip route 192.168.1.1 255.255.255.255 30.1.1.2
Device2(config)#ip route 100.1.1.1 255.255.255.255 20.1.1.1
```

#Configure Device3: Configure two static routes to the network 100.1.1.1/32. The management distance of the route with the gateway 30.1.1.1 is 10, making it become the floating route.

```
Device3#configure terminal
Device3(config)#ip route 100.1.1.1 255.255.255.255 vlan 2 10.1.1.1
Device3(config)#ip route 100.1.1.1 255.255.255.255 vlan 3 30.1.1.1 10
```

Step 3: Configure the routing policy.

#Configure Device1: configure route-map to call the ACL only matching 192.168.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface gigabitethernet1 and the next-hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfrr_static
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface gigabitethernet1 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#Configure Device3: configure route-map to call the ACL only matching 100.1.1.1/32, while the other network is filtered. The route matching the match rule

applies the backup next-hop interface gigabitethernet1 and the next-hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfrr_static
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface gigabitethernet1 backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure the fast re-routing.

#Configure Device1 to enable the fast re-routing of the static route.

```
Device1(config)#ip route static fast-reroute route-map ipfrr_static
```

#Configure Device3 to enable the fast re-routing of the static route.

```
Device3(config)#ip route static fast-reroute route-map ipfrr_static
```

Step 5: Check the result.

#View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.1.1.0/24 is directly connected, 00:31:17, vlan2
L   10.1.1.1/32 is directly connected, 00:31:17, vlan2
C   20.1.1.0/24 is directly connected, 00:08:43, vlan3
L   20.1.1.1/32 is directly connected, 00:08:43, vlan3
C   127.0.0.0/8 is directly connected, 24:43:25, lo0
L   127.0.0.1/32 is directly connected, 24:43:25, lo0
LC   100.1.1.1/32 is directly connected, 00:00:03, vlan 4
S   192.168.1.1/32 [1/10] via 10.1.1.2, 00:19:12, vlan2
```

#View the fast re-route table of Device1. You can see the route of the network 192.168.1.1/32 and the next-hop interface is gigabitethernet1.

```
Device1#show ip frr 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, E - IRMP, EX - IRMP external
S   192.168.1.1/32 [1/10] via 20.1.1.2, 00:00:10, vlan3
```

#View the backup next-hop information of Device1 and you can see that the backup interface of the fast re-routing is gigabitethernet1.

```
Device1#show nexthop frr detail
Index               : 223
Type                : FRR
Reference Count     : 1
Active Path         : master
Nexthop Address     : 10.1.1.2
Interface           : vlan2
Interface Vrf       : global
Channel ID          : 10
Link Header Length  : 18
Link Header         : 01017a12345320120101010181000000010800
Action              : FORWORDING
Slot                : 0
BK Nexthop Address  : 20.1.1.2
BK Interface        : vlan3
BK Interface Vrf    : global
BK Channel ID       : 11
BK Link Header Length  : 18
BK Link Header      : 01017a45544920120101010281000000020800
BK Action           : FORWORDING
BK Slot             : 0
Total 1 entries.
```

#After the line between Device1 and Device3 fails, the system can fast detect and switch to Device2 for communication. View the route table and fast re-route table of Device1. The egress interface to the destination network 192.168.1.1/32 in the route table is switched to the backup interface gigabitethernet1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.1.1.0/24 is directly connected, 00:31:17, vlan2
L   10.1.1.1/32 is directly connected, 00:31:17, vlan2
C   20.1.1.0/24 is directly connected, 00:08:43, vlan3
L   20.1.1.1/32 is directly connected, 00:08:43, vlan3
C   127.0.0.0/8 is directly connected, 24:43:25, lo0
L   127.0.0.1/32 is directly connected, 24:43:25, lo0
LC   100.1.1.1/32 is directly connected, 00:00:03, vlan 4
```

```
S   192.168.1.1/32 [10/10] via 20.1.1.2, 00:00:12, vlan3
```

The processing mode of Device3 is similar to Device1.

6.4 IPv6 Static Routes

6.4.1 Overview

IPv6 static routing protocol and static routing protocol have the same behaviors except the IP address structure in the packet. Refer to the introduction of static routing.

6.4.2 IPv6 Static Routing Function Configuration

Table 527 IPv6 static route configuration function list

Configuration Tasks	
Configure an IPv6 static route.	Configure an IPv6 static route.
Configure IPv6 load balancing routes.	Configure IPv6 load balancing routes.
Configure an IPv6 floating route.	Configure an IPv6 floating route.
Configure an IPv6 static route to coordinate with Track.	Configure an IPv6 static route to coordinate with Track.

6.4.2.1 Configure an IPv6 Static Route

Configuration Condition

Before configuring an IPv6 static route, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.
- Interface IPv6 addresses have been configured so that neighbor nodes are reachable at the network layer.

Configure an IPv6 Static Route

According to the parameters that have been specified, IPv6 static routes are divided 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.

The configured IPv6 static routes become invalid if some of the following conditions are met:

1. The destination address is the local interface address.
2. The administrative distance of the route is 255.
3. The output interface of the route is DOWN.
4. The egress interface of the route does not enable IPv6.
5. The gateway address is not reachable.
6. The gateway address conflicts with the local address.
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".

If an interface route meets any one condition among 1, 2, 3, 4, 8, and 9, the route is invalid. If a gateway route meets any one condition among 1, 2, 5, 6, and 9, the route is invalid. If an interface gateway route meets any of the above conditions, the route is invalid.

Table 528 Configuring an IPv6 static route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure an IPv6 static route.	ipv6 route *destination-ipv6-address/destination-mask* { *interface-name* / [*nexthop-ipv6-address*] } [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

- When configuring the default route, the destination network and mask must be set to 0::/0.
- The output interface of the Null0 route should be configured to Null0.
- The output interface of the Null0 interface need not be configured with an IPv6 address.

6.4.2.2 Configure IPv6 Load Balancing Routes

Configuration Condition

None

Configure IPv6 Load Balancing Routes

IPv6 load balancing route means that there are multiple routes 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 529 Configuring IPv6 load balancing routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the IPv6 first load balancing route.	ipv6 route *destination-ipv6-address/destination-mask interface-name1 distance*	Mandatory The output interface is interface-name1.
Configure the IPv6 second load balancing route.	ipv6 route *destination-ipv6-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.

6.4.2.3 Configure IPv6 Floating Route

Configuration Condition

None

Configure an IPv6 Floating Route

IPv6 floating static route indicates there are multiple routes 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 530 Configuring a floating route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure the IPv6 primary route.	ipv6 route *destination-ipv6-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 IPv6 floating route.	ipv6 route *destination-ipv6-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, the smaller the *distance* value is, the higher the priority is.

6.4.2.4 Configure IPv6 Static Route to Coordinate with Track

Configuration Condition

None

Configure an IPv6 Static Route to Coordinate 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 531 Configuring an IPv6 static route to coordinate 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 By default, the track object is not configured to monitor the link status of the specified interface.
Return to the global	exit	-

Step	Command	Description
configuration mode.		
Configure a static route and associate it with the Track object.	Ipv6 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.

6.4.2.5 Configure Fast Re-routing of IPv6 Static Route

Configuration Conditions

Before configuring the fast re-routing of the IPv6 static route, first complete the following task:

- When configuring the fast re-routing based on route-map, the associated route-map is already configured.

Configure Fast Re-routing of Static Route

In the network using IPv6 static routing, the traffic interruption caused by link or device failure will continue until the protocol detects the link failure and the floating route takes effect. The time often lasts for several seconds. In order to reduce the traffic interruption time, fast rerouting of the static route can be configured. By applying the route map, set the backup next hop for the successfully matched route. Once the active link fails, the traffic passing through the active link will be immediately switched to the standby link, so as to realize fast switching.

Table 532 Configure the fast re-routing of the IPv6 static route

Step	Command	Description
Enter the system configuration mode	configure terminal	-
Configure the fast re-	ipv6 route static fast-reroute	Mandatory

routing of the static route based on route-map	route-map *map-name*	By default, do not enable the fast re-routing.
Configure the auto fast re-routing of the static route	ipv6 route static pic	Mandatory' By default, do not enable auto fast re-routing.

Note

- Only the static routes specified with both out interface and gateway address can be rerouted quickly.
- Fast re-route based on route-map **set backup-nexthop** is auto, the protocol automatically reroutes fast.
- When the pic mode is used, the protocol automatically reroutes quickly.
- The various modes of enabling fast reroute are mutually exclusive.

6.4.2.6 IPv6 Static Route Monitoring and Maintaining

Table 533 IPv6 static route monitoring and maintaining

Command	Description
show ipv6 route [vrf vrf-name] static	Display the IPv6 static routes in the routing table.
show ipv6 static route [*ipv6-address*/*mask-length*]	Display the IPv6 static route.
show running-config ipv6 route	Display the configuration information about IPv6 static routes.

6.4.3 Typical Configuration Examples of IPv6 Static Route

6.4.3.1 Configure Basic Functions of IPv6 Static Route

Network Requirements

- Device1, Device2, and Device3 configure the IPv6 static route, making PC1 and PC2 communicate with each other.

Network Topology

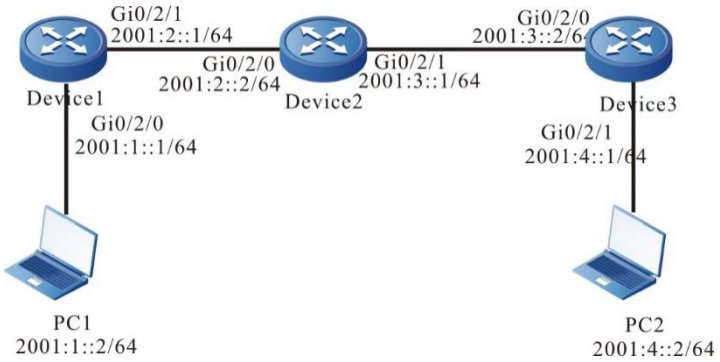


Figure 99 Networking for configuring the basic functions of the IPv6 static route

Configuration Steps

Step 1: Configure the IPv6 address of the interface (omitted).

Step 2: Configure the IPv6 static route.

#Configure the IPv6 route on Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route 2001:4::/64 2001:2::2
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route 2001:1::/64 2001:2::1
Device2(config)#ipv6 route 2001:4::/64 2001:3::2
```

#On Device3, configure the IPv6 route.

```
Device3#configure terminal
Device3(config)#ipv6 route 2001:1::/64 2001:3::1
```

#Query the IPv6 route 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

S   2001:4::/64 [1/10]
    via 2001:2::2, 00:03:14, gigabitethernet0/2/1
L   ::1/128 [0/0]
    via ::, 2w0d:01:09:06, lo0
C   2001:1::/64 [0/0]
    via ::, 00:25:55, gigabitethernet0/2/0
L   2001:1::1/128 [0/0]
    via ::, 00:25:53, lo0
C   2001:2::/64 [0/0]
    via ::, 04:01:46, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
    via ::, 04:01:45, lo0
```

#Query the IPv6 route 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 ::, 5w2d:23:52:04, lo0
S   2001:1::/64 [1/10]
    via 2001:2::1, 00:02:56, gigabitethernet0/2/0
C   2001:2::/64 [0/0]
    via ::, 04:00:52, gigabitethernet0/2/0
L   2001:2::2/128 [0/0]
    via ::, 04:00:50, lo0
C   2001:3::/64 [0/0]
    via ::, 04:00:20, gigabitethernet0/2/1
L   2001:3::1/128 [0/0]
    via ::, 04:00:19, lo0
S   2001:4::/64 [1/10]
    via 2001:3::2, 00:02:36, gigabitethernet0/2/1
```

#Query the IPv6 route 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

S   2001:1::/64 [1/10]
    via 2001:3::1, 00:00:08, gigabitethernet0/2/0
L   ::1/128 [0/0]
    via ::, 1w2d:20:54:36, lo0
C   2001:3::/64 [0/0]
    via ::, 03:58:28, gigabitethernet0/2/0
L   2001:3::2/128 [0/0]
    via ::, 03:58:26, lo0
C   2001:4::/64 [0/0]
    via ::, 00:11:13, gigabitethernet0/2/1
L   2001:4::1/128 [0/0]
    via ::, 00:11:12, lo0
```

Step 3: Check the result. Use the ping command to check the connectivity of PC1 and PC2.

#On PC1, use the ping command to check the connectivity.

```
C:\Documents and Settings\Administrator>ping 2001:4::2
Pinging 2001:4::2 with 32 bytes of data:
Reply from 2001:4::2: bytes=32 time<1ms TTL=128
Reply from 2001:4::2: bytes=32 time<1ms TTL=128
Reply from 2001:4::2: bytes=32 time<1ms TTL=128
Reply from 2001:4::2: bytes=32 time<1ms TTL=128
Ping statistics for 2001:4::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.

6.4.3.2 Configure IPv6 Static Floating Route

Network Requirements

- On Device1, configure two static routes to the segment 2001:3::/64: one is reachable via Device2, and the other is reachable via Device3.
- Device1 first uses the line with Device2 to forward the packet. When the line fails, switch to Device3 for communication.

Network Topology

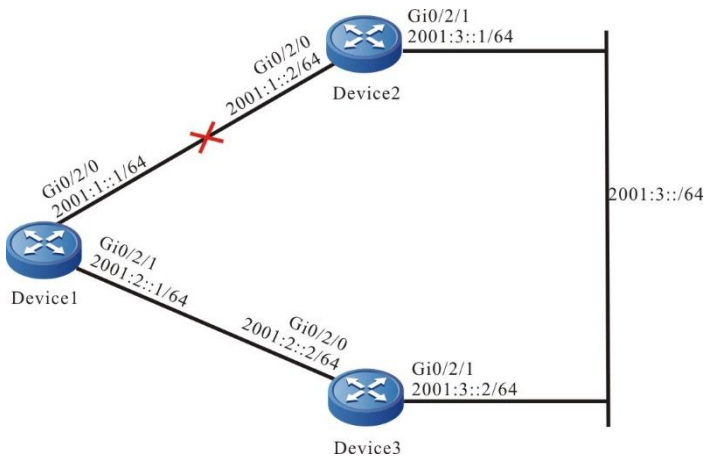


Figure 100 Networking for configuring the IPv6 static floating route

Configuration Steps

Step 1: Configure the IPv6 address of the interface (omitted).

Step 2: Configure the IPv6 static route.

#On Device1, configure two IPv6 static routes to the segment 2001:3::/64 passing Device2 and Device3 respectively.

```
Device1#configure terminal
Device1(config)#ipv6 route 2001:3::/64 2001:1::2
Device1(config)#ipv6 route 2001:3::/64 2001:2::2
```

#Query the IPv6 route 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 ::, 2w0d:02:13:16, lo0
C   2001:1::/64 [0/0]
     via ::, 00:22:33, gigabitethernet0/2/0
L   2001:1::1/128 [0/0]
     via ::, 00:22:32, lo0
C   2001:2::/64 [0/0]
     via ::, 00:17:47, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
```

```
    via ::, 00:17:46, lo0
S   2001:3::/64 [1/10]
    via 2001:1::2, 00:01:47, gigabitethernet0/2/0
          [1/10]
    via 2001:2::2, 00:01:36, gigabitethernet0/2/1
```

You can see that there are two routes to segment 2001:3::/64 on Device1, forming the load balance.

Step 3: Configure the IPv6 floating route.

#Configure Device1, modify the management distance of the route with the gateway 2001:2::2 as 15, making it become floating route.

```
Device1(config)#ipv6 route 2001:3::/64 2001:2::2 15
```

Step 4: Check the result.

#Query the IPv6 route 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 ::, 2w0d:02:16:38, lo0
C   2001:1::/64 [0/0]
    via ::, 00:25:56, gigabitethernet0/2/0
L   2001:1::1/128 [0/0]
    via ::, 00:25:55, lo0
C   2001:2::/64 [0/0]
    via ::, 00:21:10, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
    via ::, 00:21:09, lo0
S   2001:3::/64 [1/10]
    via 2001:1::2, 00:05:10, gigabitethernet0/2/0
```

In the IPv6 route table, you can see that the route with the management distance 1 is prior to the route with the management distance 15, so the route with the gateway 2001:2::2 is deleted.

#After the line between Device1 and Device2 fails, query the route 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 ::, 2w0d:02:21:06, lo0
C   2001:2::/64 [0/0]
     via ::, 00:25:38, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
     via ::, 00:25:37, lo0
S   2001:3::/64 [15/10]
     via 2001:2::2, 00:00:05, gigabitethernet0/2/1
```

In the IPv6 route table, you can see that the route with the larger management distance is added to the route table, and Device3 forwards the data.

Note

- The largest feature of the static floating route is that it can back up the route.

6.4.3.3 Configure IPv6 Static NULL0 Interface Route

Network Requirements

- On Device1 and Device2, configure one static default route respectively, and the gateway addresses are the peer interface addresses of the two devices. On Device1, configure the static Null0 interface route, and can filter the data to PC2.

Network Topology

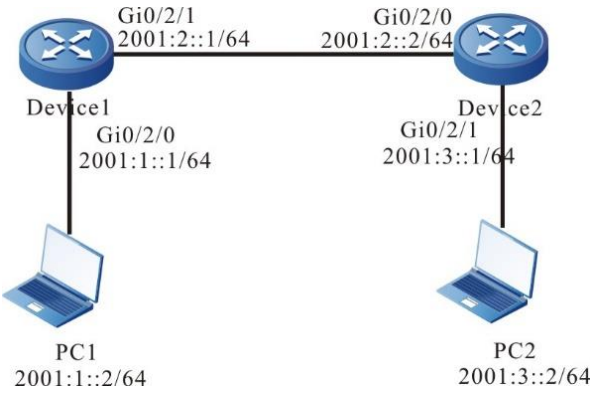


Figure 101 Networking for configuring IPv6 static NULL0 interface route

Configuration Steps

Step 1: Configure the IPv6 address of the interface (omitted).

Step 2: Configure the IPv6 static route.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route ::/0 2001:2::2
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route ::/0 2001:2::1
```

#On PC1, use the ping command to check the connectivity.

```
C:\Documents and Settings\Administrator>ping 2001:3::2
Pinging 2001:3::2 with 32 bytes of data:
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Reply from 2001:3::2: bytes=32 time<1ms TTL=128
Ping statistics for 2001:3::2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 3: Configure the IPv6 static Null0 interface route.

#Configure Device1.

```
Device1(config)#ipv6 route 2001:3::2/128 null0
```

Step 4: Check the result.

#Query the IPv6 route 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

S   ::/0 [1/10]
     via 2001:1::2, 00:04:55, gigabitethernet0/2/1
L   ::1/128 [0/0]
     via ::, 2w0d:03:36:10, lo0
C   2001:1::/64 [0/0]
     via ::, 00:08:54, gigabitethernet0/2/1
L   2001:1::1/128 [0/0]
     via ::, 00:08:53, lo0
C   2001:2::/64 [0/0]
     via ::, 00:08:32, gigabitethernet0/2/0
L   2001:2::1/128 [0/0]
     via ::, 00:08:30, lo0
S   2001:3::2/128 [1/1]
     via ::, 00:00:34, null0
```

In the Ipv6 route table, the IPv6 static Null0 interface route is added.

#On PC1, use the ping command to check the connectivity with PC2.

```
C:\Documents and Settings\Administrator>ping 2001:3::2
Pinging 2001:3::2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2001:3::2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After searching for the route table for the ICMP packet sent by PC1 on Device1, discover that the egress interface is Null0, and directly drop. Therefore, PC1 cannot communicate with PC2.

Note

- The static Null0 interface route is one special route, and the packets sent to the Null0 interface are all dropped. Therefore, configuring the static Null0 interface route can realize the filtering for the packets.

6.4.3.4 Configure IPv6 Static Recursive Route

Network Requirements

- On Device1, configure two static routes to the segment 192::3/128: one is reachable via Device2, and the other is reachable via Device3. Device1 first uses the line with Device3 to forward the packet.
- On Device1, configure one static recursive route to the segment 2001:4::/64, and the gateway address is the loopback interface address of Device3 192::3. After the line between Device1 and Device3 fails, the route can switch to Device2 for communication.

Network Topology

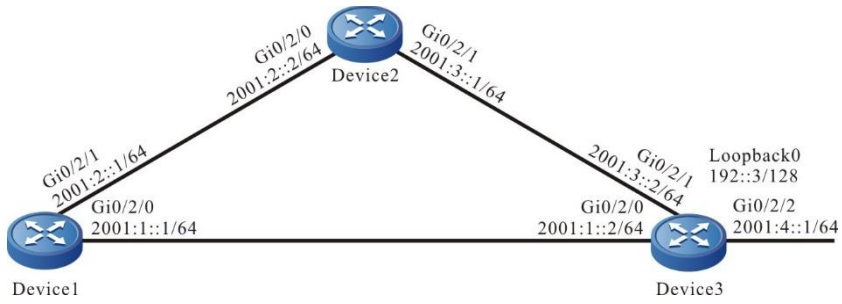


Figure 102 Networking for configuring IPv6 static recursive route

Configuration Steps

Step 1: Configure the IPv6 address of the interface (omitted).

Step 2: Configure the IPv6 static route.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 route 192::3/128 2001:1::2
```

```
Device1(config)#ipv6 route 192::3/128 2001:2::2 10
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 route 192::3/128 2001:3::2
```

Step 3: Configure the IPv6 static recursive route.

Configure Device1.

```
Device1(config)#ipv6 route 2001:4::/64 192::3
```

#Query the IPv6 route 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 ::, 2w0d:03:12:46, lo0
S   192::3/128 [1/10]
     via 2001:1::2, 00:04:54, gigabitethernet0/2/0
C   2001:1::/64 [0/0]
     via ::, 00:22:47, gigabitethernet0/2/0
L   2001:1::1/128 [0/0]
     via ::, 00:22:45, lo0
C   2001:2::/64 [0/0]
     via ::, 00:16:16, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
     via ::, 00:16:15, lo0
S   2001:4::/64 [1/10]
     via 192::3, 00:00:43, gigabitethernet0/2/0
```

In the IPv6 route table, you can see that the gateway address of the route 2001:4::/64 is 192::3, the egress interface is gigabitethernet0/2/0, and the route depends on the route 192::3/128.

Step 4: Check the result.

#After the line between Device1 and Device3 fails, query the IPv6 route 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 ::, 2w0d:03:17:48, lo0
S   192::3/128 [10/10]
    via 2001:2::2, 00:00:06, gigabitethernet0/2/1
C   2001:2::/64 [0/0]
    via ::, 00:21:18, gigabitethernet0/2/1
L   2001:2::1/128 [0/0]
    via ::, 00:21:17, lo0
S   2001:4::/64 [1/10]
    via 192::3, 00:00:06, gigabitethernet0/2/1
```

6.4.3.5 Compared with the route table of step 3, you can see that the egress interface of the route 2001:4::/64 is gigabitethernet0/2/1, indicating that the route already switches to Device2 for communication. Configure Static Fast Re-routing of IPv6 Static Route

Network Requirements

- Device1 is configured with two static routes to the destination network segment 1001:2::1/64. One is reachable through Device2 and the other is reachable through Device3. Device1 preferentially uses the line with Device2 to forward packets.
- Static fast rerouting is enabled between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

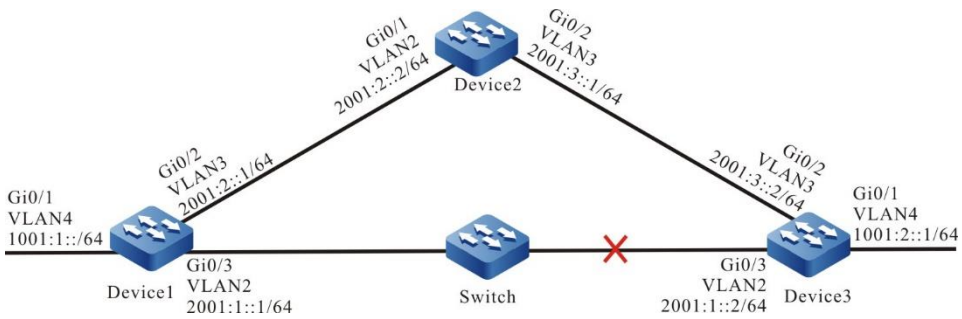


Figure 103 Networking of configuring the static fast re-routing of IPv6 static route

Configuration Steps

Step 1: Configure VLAN, add the port to the corresponding VLAN; configure the IPv6 route of the interface (omitted).

Step 2: Configure the IPv6 static route.

#Configure Device1, and configure two statuc routes to the 1001:2::/64 network.

```
Device1#configure terminal
Device1(config)#ipv6 route 1001:2::/64 vlan2 2001:1::2
Device1(config)#ipv6 route 1001:2::/64 vlan3 2001:2::2 10
```

#Configure Device2, and configure one static route to the 1001:2::1/64 network.

```
Device2#configure terminal
Device2(config)#ipv6 route 1001:2::/64 vlan3 2001:3::2
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next hop interface vlan3, and the next hop address 2001:2:: 2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_st
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-nexthop 2001:2::2
Device1(config-route-map)#exit
```

Step 4: Configure the static fast re-routing.

```
Device1(config)#ipv6 route static fast-reroute route-map ipv6frr_st
```

Step 5: Check the result.

#View the IPv6 static route 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 ::, 04:26:25, lo0
C   1001:1::/64 [0/0]
    via ::, 04:21:32, vlan4
L   1001:1::1/128 [0/0]
    via ::, 04:21:32, vlan4
S   1001:2::/64 [1/10]
    via 2001:1::2, 00:03:00, vlan2
C   2001:1::/64 [0/0]
    via ::, 04:22:11, vlan2
L   2001:1::1/128 [0/0]
    via ::, 04:22:11, vlan2
C   2001:2::/64 [0/0]
    via ::, 04:20:50, vlan3
L   2001:2::1/128 [0/0]
    via ::, 04:20:50, vlan3
```

It can be seen from the routing table that route 1001:2:: / 64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 frr route table of Device1.

```
Device1#show ipv6 frr 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
S   1001:2::/64 [1/4294967295]
    via 2001:2::2, 00:04:32, vlan3
```

You can see that the next hop of the frr route 1001:2::/64 is 2001:2::2, and the out interface is gigabitethernet1.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6  2001:1::2  detail
Total ipv6 session number: 1
OurAddr          NeighAddr        LD/RD              State     Holddown    Interface
2001:1::1        2001:1::1        1015/1015          UP        500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:67  Remote Discriminator:67
Local State:UP  Remote State:UP  Up for: 0h:30m:28s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
```

```
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is set up normally and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2:: / 64 has been switched to the backup interface gigabitethernet1.

```
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 ::, 04:56:34, lo0
C   1001:1::/64 [0/0]
    via ::, 04:51:41, vlan4
L   1001:1::1/128 [0/0]
    via ::, 04:51:41, vlan4
S   1001:2::/64 [10/10]
    via 2001:2::2, 00:00:08, vlan3
C   2001:2::/64 [0/0]
    via ::, 04:50:59, vlan3
L   2001:2::1/128 [0/0]
    via ::, 04:50:59, vlan3
```

6.4.3.6 Configure Dynamic Fast Re-routing of IPv6 Static Route

Network Requirements

- Device1 is configured with two static routes to the destination network segment 1001:2::1/64. One is reachable through Device2 and the other is reachable through Device3. Device1 preferentially uses the line with Device2 to forward packets.
- Dynamic fast rerouting is enabled between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for

communication.

Network Topology

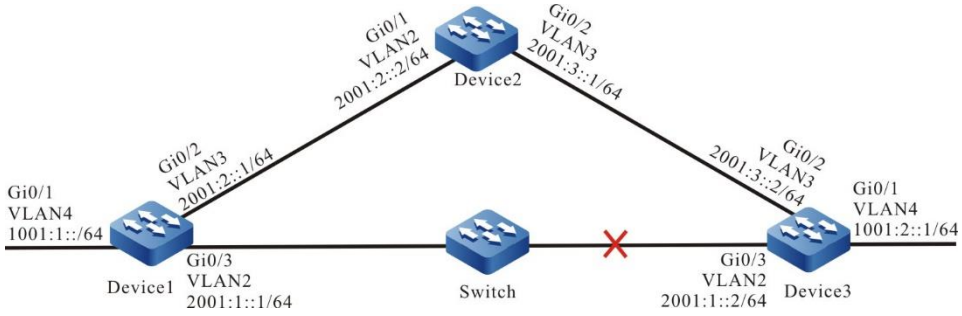


Figure 104 Networking of configuring the dynamic fast re-routing of IPv6 static route

Configuration Steps

Step 1: Configure the IPv6 route of the interface (omitted).

Step 2: Configure the IPv6 static route.

#Configure Device1, and configure two statuc routes to the 1001:2::/64 network.

```
Device1#configure terminal
Device1(config)#ipv6 route 1001:2::/64 vlan2 2001:1::2
Device1(config)#ipv6 route 1001:2::/64 vlan3 2001:2::2 10
```

#Configure Device2, and configure one static route to the 1001:2::1/64 network.

```
Device2#configure terminal
Device2(config)#ipv6 route 1001:2::/64 vlan3 2001:3::2
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next hop interface gigabitethernet1, and the next hop address is auto.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_st
Device1(config-route-map)#match ipv6 address 7001
```

```
Device1(config-route-map)#set ipv6 fast-reroute backup-nexthop auto
Device1(config-route-map)#exit
```

Step 4: Configure the dynamic fast re-routing.

```
Device1(config)#ipv6 route static fast-reroute route-map ipv6frr_st
```

Step 5: Check the result.

#View the IPv6 static route 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 ::, 04:26:25, lo0
C   1001:1::/64 [0/0]
    via ::, 04:21:32, vlan4
L   1001:1::1/128 [0/0]
    via ::, 04:21:32, vlan4
S   1001:2::/64 [1/10]
    via 2001:1::2, 00:03:00, vlan2
C   2001:1::/64 [0/0]
    via ::, 04:22:11, vlan2
L   2001:1::1/128 [0/0]
    via ::, 04:22:11, vlan2
C   2001:2::/64 [0/0]
    via ::, 04:20:50, vlan3
L   2001:2::1/128 [0/0]
    via ::, 04:20:50, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 frr route table of Device1.

```
Device1#show ipv6 frr 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
S   1001:2::/64 [1/4294967295]
    via 2001:2::2, 00:04:32, vlan3
```

You can see that the next hop of the frr route 1001:2::/64 is 2001:2::2, and the out interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6  2001:1::1  detail
Total ipv6 session number: 1
OurAddr          NeighAddr         LD/RD              State     Holddown    Interface
2001:1::1        2001:1::1         1012/1012          UP        500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:67  Remote Discriminator:67
Local State:UP  Remote State:UP  Up for: 0h:30m:28s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is set up normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2:: / 64 has been switched to the backup interface gigabitethernet1.

```
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 ::, 04:56:34, lo0
C   1001:1::/64 [0/0]
     via ::, 04:51:41, vlan4
L   1001:1::1/128 [0/0]
     via ::, 04:51:41, vlan4
S   1001:2::/64 [10/10]
     via 2001:2::2, 00:00:08, vlan3
C   2001:2::/64 [0/0]
     via ::, 04:50:59, vlan3
L   2001:2::1/128 [0/0]
     via ::, 04:50:59, vlan3
```

6.5 RIP

6.5.1 Overview

On the current Internet, it is impossible to run only one gateway protocol. You can divide it into multiple Autonomous Systems (ASs) and each 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 route 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.

6.5.2 RIP Function Configuration

Table 534 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.
	Configure RIP to re-distribute routes.

Configuration Tasks	
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.
Configure RIP to coordinate with BFD.	Configure RIP to coordinate with BFD.

6.5.2.1 Configure Basic Functions of RIP

Configuration Condition

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 535 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.
- The **network** *ip-address* command cannot cover the 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 536 Enable RIP for VRF

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.
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 537 Configure RIP versions

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
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.

6.5.2.2 Configure RIP Route Generation

Configuration Condition

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 538 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 {only | originate [metric *value*] }	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 loops 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 Redistribute Routes

By redistributing routes, you can introduce the routes generated by other protocols to RIP.

Table 539 Configure RIP to redistribute 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.
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 redistribute routes.	redistribute *protocol* [*protocol-id*] [metric *metric-value*] [route-map *route-map-name*] [match *route-sub-type*]	Mandatory. By default, route redistribution is not configured.

Note

- If the metric command option is specified during redistribution, the redistributed route adopts the metric.
- In configuring RIP to redistribute routes, the available *match* options for the applied routing policy include ip address, route type, and tag, and the

available set options for the applied routing policy include interface, ip next-hop, route source, and metric.

6.5.2.3 Configure RIP Route Control

Configuration Condition

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 540 Configure the administrative distance of RIP

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

After RIP route summary is configured, the device advertises only the route summary. This greatly decreases the size of adjacent RIP route 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 541 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.	auto-summary	Mandatory. By default, the auto route summary function is disabled.

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 542 Configure the manual route summary function

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

Step	Command	Description
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 route 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 543 Configure 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 544 Configure 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 filtering function.	distribute-list { *access-list-name* | prefix *prefix-list-name* } { in | out } [*interface-name*]	Mandatory. By default, the route filtering function is not configured. During the configuration process of the route filtering function, if no interface is specified, route filtering is 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 Metric of 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 545 Configure 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 routing policy, the network administrator can perform route filtering or route property advertisement based on the tags.

Only the routing tags of RIPv2 are supported.

Table 546 Configure 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 547 Configure 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	maximum-paths *max-*	Optional.

Step	Command	Description
RIP load balancing entries.	*number*	By default, the maximum number of RIP load balancing entries is 4.

6.5.2.4 Configure RIP Network Authentication

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 548 Configure 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 | sm3} } }	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.

6.5.2.5 Configure RIP Network Optimization

Configuration Condition

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 549 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.

Caution

- 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 550 Configure 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 551 Configure RIP toxicity reverse

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

Step	Command	Description
Configure RIP toxicity reverse.	ip split-horizon poisoned	Optional. By default, the toxicity reverse function is enabled.

Caution

- The split horizon and toxicity reverse functions are valid only for the learnt routes, direct routes in the network covered by RIP, and the redistributed 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 552 Configure 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 553 Configure 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	neighbor *ip-address*	Mandatory.

routes to a neighbor in unicast mode.		The parameter *ip-address* is the IP address of the peer direct-connect interface.

Caution

- 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 554 Configure 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.

Caution

- 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 route 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 555 Configure 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 route table, and advertises the local route 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 556 Configure 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.

6.5.2.6 Configure RIP to Coordinate with BFD

A backup interface can be used only in a specific application environment, but it cannot meet the real-time backup requirement. At this time, RIP provides the point-to-point Bidirectional Forwarding Detection (BFD) function to realize fast convergence and switchover of routes. BFD provides a method for quickly detecting the status of a

line between two devices. When BFD detection is enabled between two adjacent RIP devices, if the line between the two devices is faulty, BFD can quickly find the fault and notify RIP. RIP then deletes the RIP route that is associated with the BFD interface. If the route has a backup route, a switchover to the backup route will be performed in a very short period of time (which is determined by BFD settings). Currently, RIP only supports single-hop bi-directional BFD detection.

Table 557 Configure RIP to coordinate with BFD

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.
Enable the BFD function on all the interfaces that are covered by the RIP process.	bfd all-interfaces	Mandatory. By default, the BFD function is disabled on all the interfaces that are covered by the RIP process.
Return to the global configuration mode.	exit	-
Enter the interface configuration mode.	interface *interface-name*	-
Enable the BFD function on the interface.	ip rip bfd	Mandatory. By default, the BFD function is disabled on the interface.

Caution

- For the related configuration of BFD, refer to Reliability- BFD technical manual.

6.5.2.7 RIP Monitoring and Maintaining

Table 558 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 }	Clear RIP process and statistics.

6.5.3 RIP Typical Configuration Example

6.5.3.1 Configure RIP Version

Network Requirements

- RIPv2 runs between Device1 and Device2 for route interaction.

Network Topology

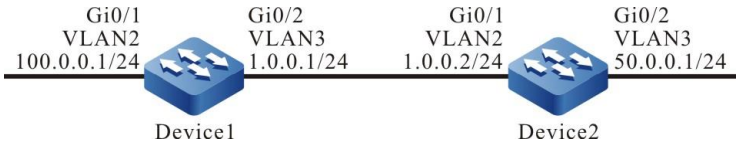


Figure 105 Networking for configuring the RIP version

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

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 route table, the route advertised by the device uses a 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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

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 100.0.0.0/24 [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 route table, the route advertised by the device uses a 24-bit accurate mask.

6.5.3.2 Configure RIP to Redistribute Routes

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 redistributes OSPF route 100.0.0.0/24 to RIP and advertises the route to Device3.

Network Topology

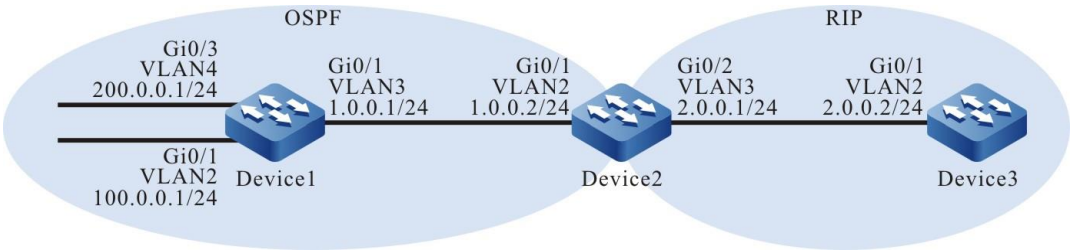


Figure 106 Networking for configuring RIP to redistribute routes

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external
C   1.0.0.0/24 is directly connected, 00:23:06, vlan2
C   2.0.0.0/24 is directly connected, 00:13:06, vlan3
O   100.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
C   127.0.0.0/8 is directly connected, 76:51:00, lo0
O   200.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
```

According to the route 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 routing 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)#commit
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 routing 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 redistribute 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 route 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 route table of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external

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 route table on Device2 and the querying the route table on Device3, it is found that route 100.0.0.0/24 on Device2 has been redistributed 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 redistribute routes between different routing protocols. If route redistribution must be configured, you are required to configure route control policies such as route filtering and filtration summary on the AS boundary routers to prevent routing loops.

6.5.3.3 Configure RIP Metric Offset

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

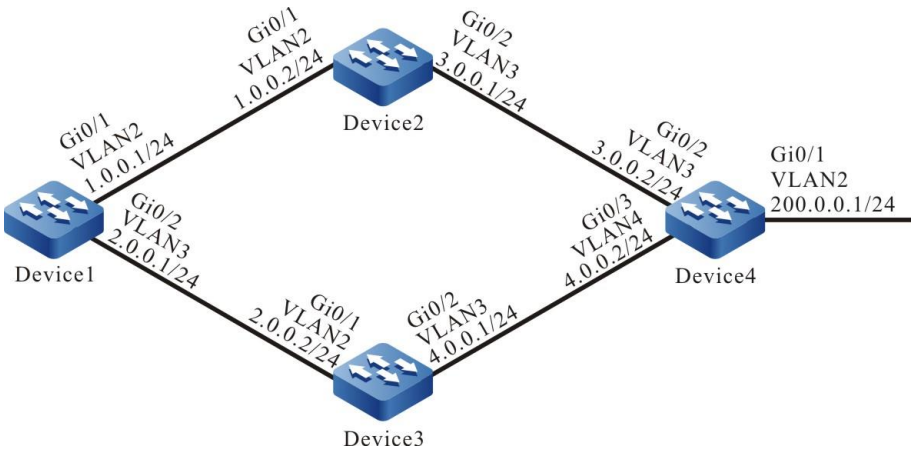


Figure 107 Networking for configuring the RIP metric offset

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route 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)#commit
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 ACL 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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route 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 receive and advertisement directions.

6.5.3.4 Configure RIP Route Filtration

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

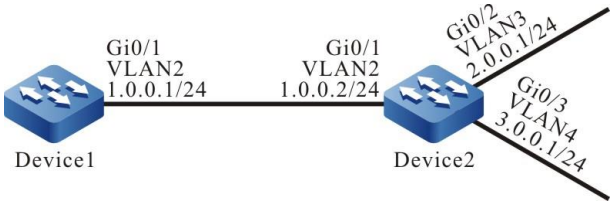


Figure 108 Networking for configuring RIP Route filtration

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
```

```
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 route 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)#commit
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 filtering 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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table, Device2 does not advertise route 3.0.0.0/24 to Device1, but the route is deleted from the route 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 receive and advertisement directions.

6.5.3.5 Configure RIP Route Summary

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 route table of Device1, it is required that Device advertises only the route summary of the two route to Device1.

Network Topology

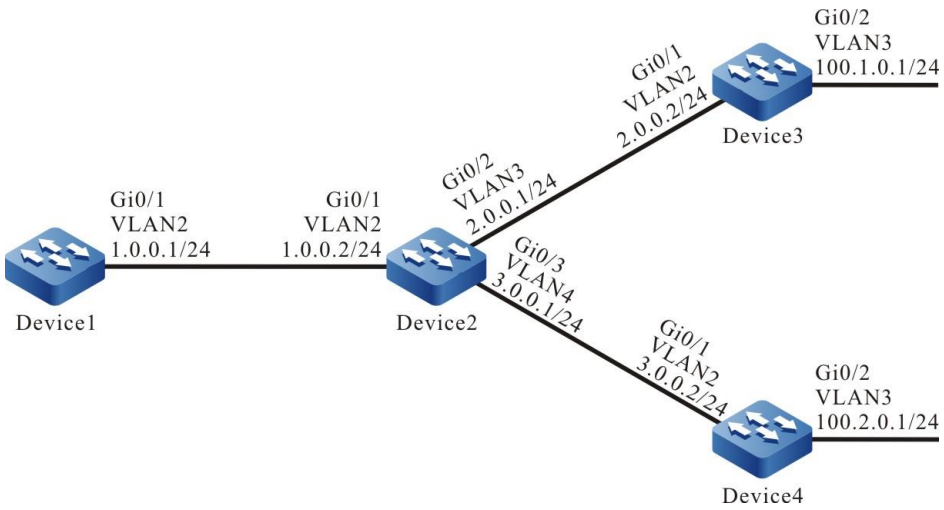


Figure 109 Networking for configuring RIP route summary

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 a 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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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.

6.5.3.6 Configure RIP to Coordinate with BFD

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.
- Configure BFD between Device1 and Device2. When the line between Device1 and Device2 becomes faulty, configure RIP to coordinate with BFD between Device1 and Device2 to quickly detect line faults. When BFD finds a main line failure, it triggers an RIP route update. Then the route 3.0.0.0/24 is switched over to the backup line.

Network Topology

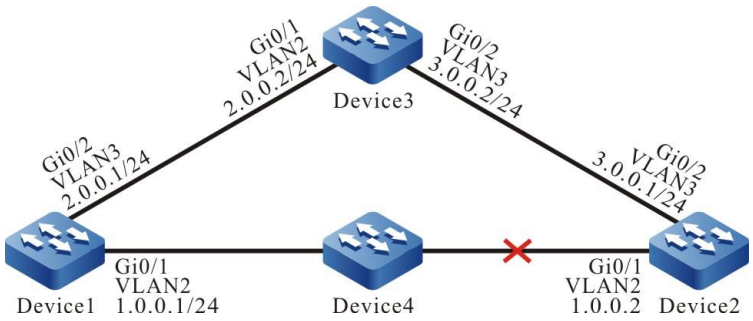


Figure 110 Networking for configuring RIP to coordinate with BFD

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 at the input direction of interface VLAN3 so that the metric of the routes that match 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-std-nacl)#commit
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 a route metric offset is configured, Device1 selects route 3.0.0.0/24 advertised by Device2.

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.

#On Device1, query the BFD information.

```
Device1#show bfd session
OurAddr          NeighAddr          LD/RD          State      Holddown      interface
1.0.0.1          1.0.0.2            2/4            UP         5000          vlan2
```

#If the line between Device1 and Device2 becomes faulty, the route can quickly switch over to the backup line.

#On Device1, query the route information.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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
```

6.5.3.7 Configure RIP Backup Interface

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

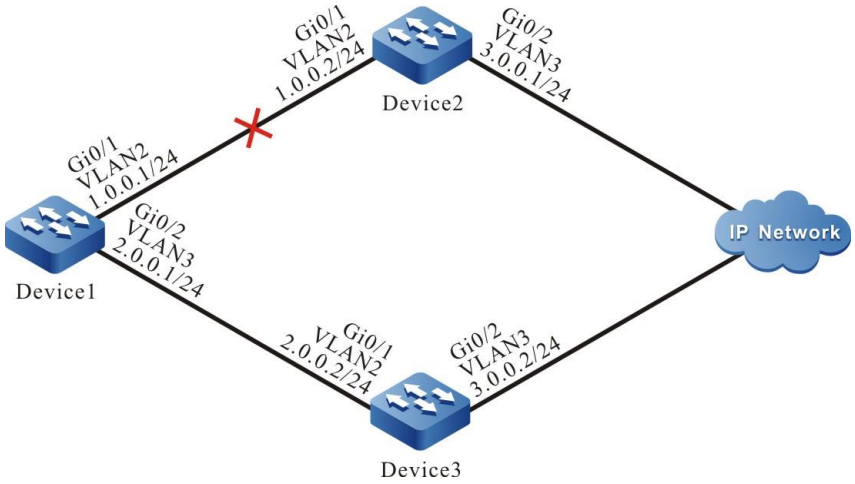


Figure 111 Networking for configuring an RIP backup interface

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 at the input direction of interface VLAN3 so that the metric of the routes that match 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-std-nacl)#commit
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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
```

6.5.3.8 Configure Passive RIP Interface

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

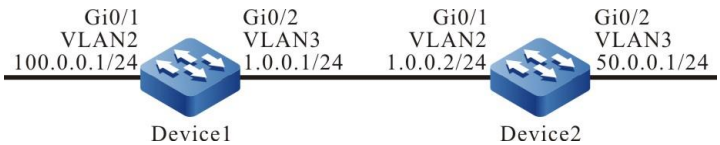


Figure 112 Networking for configuring an RIP passive interface

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external
```

```
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   100.0.0.0/24 [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 route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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 route table.

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 00:25:06, vlan2
C   50.0.0.0/24 is directly connected, 00:25:06, vlan3
C   127.0.0.0/8 is directly connected, 77:51:00, lo0
```

6.6 RIPng

6.6.1 Overview

RIPng, also known as next-generation RIP protocol, is a dynamic routing protocol used by the IPv6 networks to provide routing information for the IPv6 packet forwarding. RIPng is extended on RIP-2. The working principle of the RIPng protocol is basically the same as that of the RIP protocol. In order to adapt to the IPv6 network, RIPng has made the following changes to the original RIP protocol:

UDP port number: The RIPng protocol uses UDP port number 521 to send and receive the 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 broadcasting.

Prefix length: The destination address of the RIPng protocol route uses the 128-bit prefix length;

Next-hop address: The RIPng protocol uses 128-bit IPv6 address;

Source address: The RIPng protocol uses the link local address FE80:/10 as the source address to send the RIPng protocol packet.

The protocol specifications related to RIPng include RFC2080 and RFC2081.

6.6.2 RIPng Function Configuration

Table 559 RIPng function configuration list

Configuration Tasks	
Configure RIPng basic functions	Enables RIPng globally
Configure RIPng route generation	Configure RIPng to advertise the default route.
	Configure RIP to re-distribute routes
Configure RIPng route control	Configure the administrative distance of RIPng

Configuration Tasks	
	Configure a RIPng route summary.
	Configure the RIPng metric offset.
	Configure RIPng route filtering
	Configure the metric of the RIPng interface.
	Configure the routing flag for a RIPng interface.
	Configure the maximum load balancing for RIPng
Configure RIPng network optimization	Configure RIPng timers.
	Configure RIPng split horizon and toxicity reverse of RIP.
	Configure a RIPng static neighbor.
	Configure a RIPng passive interface.

6.6.2.1 Configure Basic Functions of RIPng

Configuration Condition

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 of the interface is enabled.

Enable RIPng Globally

Before using RIPng, make the following configurations:

- Create a RIPng process.

- Enable the RIPng protocol on the interface

Table 560 Enabling RIPng globally

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create a RIPng process and enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory. By default, the RIPng process is disabled.
Return to the global configuration mode	exit	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the RIPng protocol on the interface	ipv6 rip enable *process-id*	Mandatory By default, do not enable the RIPng protocol on the interface.

6.6.2.2 Configure RIPng Route Generation

Configuration Condition

Before configuring RIPng route generation, ensure that:

- The IPv6 capability of the interface is enabled.
- RIPng is enabled.

Configure RIPng to Advertise the Default Route

Through configuration, a device can send the default route in all RIPng interfaces to set itself as the default gateway of other neighbor devices.

Table 561 Configure RIPng to advertise the default route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory By default, the RIPng process is disabled.
Configure RIPng to advertise the default route.	default-information originate [metric *value*]	Mandatory 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 loops 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 Redistribute Routes

By redistributing routes, you can introduce the routes generated by other protocols to RIPng.

Table 562 Configure RIPng to redistribute routes

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

Step	Command	Description
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory 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 redistribute routes.	redistribute *protocol* [*protocol-id*] [metric *metric-value*] [route-map *route-map-name*] [match *route-sub-type*]	Mandatory. By default, route redistribution is not configured.

Note

- If the metric command option is specified during redistribution, the redistributed route adopts the metric.
- In configuring RIPng to redistribute routes for applying the route map, the available match options include ipv6 address, route type, tag, interface, ipv6 nexthop, ipv6 route-source, and metric, and the available set options include metric and tag.

6.6.2.3 Configure RIPng Route Control

Configuration Condition

Before configuring RIPng route control, ensure that:

- The IPv6 capability of the interface is enabled.
- 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 563 Configure the administrative distance of RIPng

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	-
Configure the administrative distance of RIPng.	distance *distance-value*	Mandatory. By default, the administrative distance of RIPng is 120.

Configure a RIPng Route Summary

RIPng route summary always indicates configuring a pair of destination addresses and masks, which summarizes the routes in the covered network segment.

After RIP route summary is configured, the device advertises only the summary route. This greatly decreases the size of adjacent RIPng route tables in the medium and large networks, and decreases the consumption of the routing protocol packets for the network bandwidth.

The metric of the summary route adopts the minimum of all subnet route metrics.

Table 564 Configure the RIPng route summary function

Step	Command	Description
Enter the 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*	Mandatory By default, do not configure the route summary function.

Configure the RIPng Metric Offset

By default, RIPng adopts the route metric advertised by the neighbor device for 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, 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 565 Configure the RIPng metric offset

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory By default, the RIPng process is disabled.
Configure RIPng to modify the	offset-list *access-*	Mandatory

Step	Command	Description
metric of the specified route.	*list-name* { in | out } *metric-offset* [*interface-name*]	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) or prefix list. In receiving RIPng routes, you can filter some learnt routes; or in advertising RIPng routes, you can filter some routes that are advertised to neighbor devices.

Table 566 Configure RIPng route filtration

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory By default, the RIPng process is disabled.
Configure the RIPng route filtering function	distribute-list { *access-list-name* | prefix *prefix-list-name* | route-map *route-map-name*} { in | out } [*interface-name*]	Mandatory By default, the route filtering function is not configured. During the configuration process of the route filtering function, if no interface is specified, route filtering is enabled for all RIPng interfaces.

Configure the Metric of the RIPng Interface

After the 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, and if the metric is configured on the interface, adopt the interface metric.

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 567 Configure the metric of the RIPng interface

Step	Command	Description
Enter the 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*	Mandatory By default, the RIPng interface metric is 1.

Note

- Configuring the RIPng interface metric affects only the metric of the direct subnet on the interface, while it does not affect the metric learned by the route.

Configure the Routing Tag for a RIPng Interface

The network administrator can attach tags to some routes. Then, when applying a routing policy, perform route filtering or route property advertisement based on the tags.

Table 568 Configure the routing flag for a RIPng interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure a RIPng route tag of the direct subnet on the interface.	ipv6 rip tag *tag-value*	Mandatory By default, do not configure the route tag.

Configure the Maximum Number of RIPng Load Balancing Entries

This command helps you to control the number of the load balancing entries of the RIPng route.

Table 569 Configure the maximum number of RIPng load balancing entries

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory 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.

6.6.2.4 Configure RIPng Network Optimization

Configuration Condition

Before configuring RIPng network optimization, ensure that:

- Configure the interface to enable the IPv6 capability
- Enable the RIPng protocol

Configure RIPng Timers

RIPng does not maintain neighbor relations and 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 570 Configuring RIPng timers

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode.	ipv6 router rip *process-id*	Mandatory By default, the RIPng process is disabled.
Configure RIPng timers	timers *update-interval invalid-interval holddown-*	Optional.

	interval flush-interval	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 120s.

Caution

- In the same RIPng routing domain, the timer configurations on all the devices must be the same to prevent network flapping.

Configure RIPng 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.

RIPng does not advertise routes that it has learnt from an interface to the interface, preventing routing loops.

Table 571 Configure RIPng split horizon

Step	Command	Description
Enter the 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 advertises the 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 572 Configure RIPng toxicity reverse

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure RIPng toxicity reverse	ipv6 split-horizon poison-reverse	Mandatory 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 the RIPng interface, and the redistributed 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 a broadcast or multicast network, it may cause repeated RIPng packets in the network.

Table 573 Configure a static RIPng neighbor

Step	Command	Description
Enter the 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*	Mandatory 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 574 Configure a passive RIPng interface

Step	Command	Description
Enter the global	configure terminal	-

configuration mode.		
Enter the interface configuration mode.	interface *interface-name*	-
Configure a passive RIPng interface.	ipv6 rip passive	Mandatory By default, no passive interface is configured.

Note

- **ipv6 rip passive** does not restrain an interface from sending unicast route updates to its neighbor devices. When being 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 can control 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 multicast mode.

6.6.2.5 Configure RIPng to Coordinate with BFD

A backup interface can be used only in a specific application environment, but it cannot meet the real-time backup requirement. At this time, RIP provides the point-to-point Bidirectional Forwarding Detection (BFD) function to realize fast convergence and switchover of routes. BFD provides a method for quickly detecting the status of a line between two devices. When BFD detection is enabled between two adjacent RIPng devices, if the line between the two devices is faulty, BFD can quickly find the fault and notify RIPng. RIP then deletes the RIPng route that is associated with the BFD interface. If the route has a backup route, a switchover to the backup route will be performed in a very short period of time (which is determined by BFD settings). Currently, RIPng only supports single-hop bi-directional BFD detection.

Table 575 Configure RIPng to coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the RIPng configuration mode	ipv6 router rip 100	Mandatory By default, do not enable the RIPng process.
Enable the BFD function on all the interfaces that are covered by the RIPng process.	bfd all-interfaces	Mandatory. By default, the BFD function is disabled on all the interfaces that are covered by the RIPng process.
Return to the global configuration mode.	exit	-
Enter the interface configuration mode.	interface *interface-name*	-
Enable the BFD function on the interface.	Ipv6 rip bfd	Mandatory. By default, the BFD function is disabled on the interface.

Note

- For the related configuration of BFD, refer to Reliability- BFD technical manual.

6.6.2.6 RIPng Monitoring and Maintaining

Table 576 RIPng monitoring and maintaining

Command	Description
clear ipv6 rip [*process-id*]{ process | statistics }	Clears the RIPng process and statistics

Command	Description
	information
show ipv6 rip [*process-id*]	Displays the RIPng protocol basic information
show ipv6 rip [*process-id*] database [detail | *ipv6-address/mask-length* [detail | longer-prefixes]]	Displays the RIPng route database information
show ipv6 rip [*process-id*] statistics [*interface-name*]	Displays the RIPng interface statistics information
show ipv6 rip interface [*interface-name*]	Displays the RIPng interface information

6.6.3 RIPng Typical Configuration Example

6.6.3.1 Configure RIPng Basic Functions

Network Requirements

Run RIPng between Device1 and Device2 for route interaction.

Network Topology

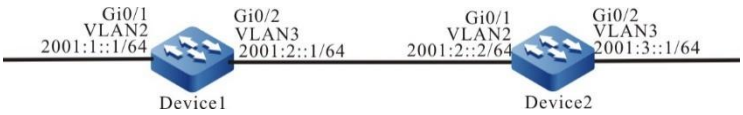


Figure 113 Networking for configuring RIPng basic functions

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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.

#View the IPv6 route 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 ::, 00:21:40, lo0
C   2001:2::/64 [0/0]
     via ::, 00:21:34, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:21:33, 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:22:39:31, lo0
R   2001:1::/64 [120/2]
     via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:30:46, vlan2
L   2001:2::2/128 [0/0]
     via ::, 00:30:45, lo0
C   2001:3::/64 [0/0]
     via ::, 00:29:12, vlan3
L   2001:3::1/128 [0/0]
     via ::, 00:29:11, lo0
```

According to the routing table, you can see that the route advertised by the device uses a 64-bit exact mask.

6.6.3.2 Configure RIPng to Redistribute Routes

Network Requirements

Run the IPv6 OSPF protocol between Device1 and Device2, Device2 learns the IPv6 OSPF route released by Device1 2001:1::/64, 2001:2::/64.

Run the RIPng protocol between Device2 and Device3, Device2 only distributes the IPv6 OSPF route 2001:1::/64 to RIPng, and advertises the route to Device3.

Network Topology

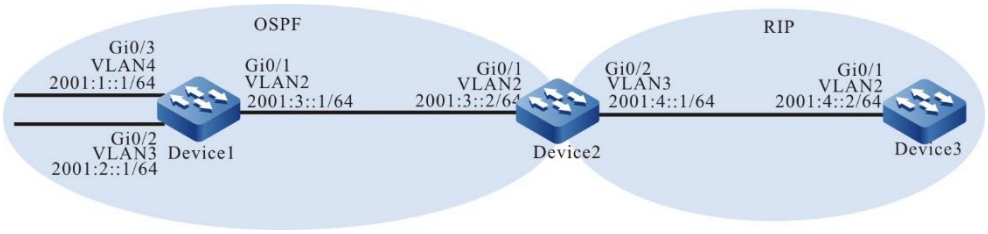


Figure 114 Networking for configuring RIPng to redistribute the route

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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 route 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:00:09:49, lo0
O    2001:1::/64 [110/2]
     via fe80::201:7aff:fe01:204, 00:12:16, vlan2
O    2001:2::/64 [110/2]
```

```
    via fe80::201:7aff:fe01:204, 00:12:16, vlan2
C   2001:3::/64 [0/0]
    via ::, 00:19:51, vlan2
L   2001:3::2/128 [0/0]
    via ::, 00:19:50, lo0
C   2001:4::/64 [0/0]
    via ::, 00:45:13, vlan3
L   2001:4::1/128 [0/0]
    via ::, 00:45:12, lo0
```

According to the routing table, you can see that Device2 has learnt the IPv6 OSPF route 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 routing policy.

#On Device2, configure route-map to invoke the 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 routing 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 redistribute IPv6 OSPF routes.

#Configure RIPng to redistribute IPv6 OSPF routes.

```
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 route 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:20:00:11, lo0
R   2001:1::/64 [120/2]
    via fe80::201:7aff:fec3:38a5, 02:50:14, vlan2
C   2001:4::/64 [0/0]
    via ::, 03:56:24, vlan2
L   2001:4::2/128 [0/0]
```

```
via ::, 03:56:23, lo0
```

By querying the database of Device2 and the route table of Device3, it is found that the route on Device2 2001:1::/64 is re-distributed to RIPng and is successfully advertised to Device3, while the route 2001:2::/64 has been successfully filtered out.

Caution

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not redistribute routes between different routing protocols. If route redistribution must be configured, you are required to configure route control policies such as route filtering and filtration summary on the AS boundary routers to prevent routing loops.

6.6.3.3 Configure RIPng Metric Offset

Network Requirements

- Device1, Device2, Device3, and Device4 runs the RIPng protocol and interconnects with each other.
- 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

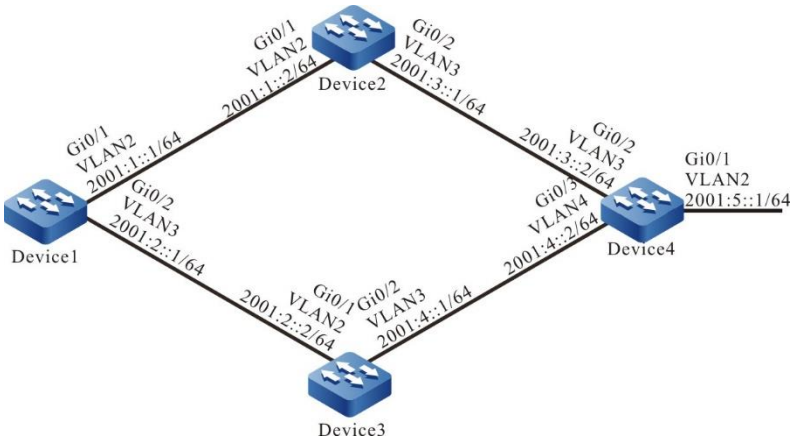


Figure 115 Networking for configuring the RIPng metric offset

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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
```

#View the IPv6 route 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:06:21:24, lo0
C   2001:1::/64 [0/0]
     via ::, 00:02:05, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:02:04, lo0
C   2001:2::/64 [0/0]
     via ::, 00:02:02, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:02:01, lo0
R   2001:3::/64 [120/2]
```

```
    via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
R   2001:4::/64 [120/2]
    via fe80::201:7aff:fe11:2214, 00:00:48, vlan3
R   2001:5::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
          [120/3]
    via fe80::201:7aff:fe11:2214, 00:00:48, vlan3
```

In the route table of Device1, you can see two routes to 2001:5::/64.

Step 4: Configure the access list.

```
Device1(config)#ipv6 access-list extended RIPng
Device1(config-v6-list)#permit 10 2001:5::/64 any
Device1(config-v6-list)#commit
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.

#View the IPv6 route 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]
06:34:28, lo0
C   2001:1::/64 [0/0]
    via ::, 00:15:09, vlan2
L   2001:1::1/128 [0/0]
    via ::, 00:15:08, lo0
C   2001:2::/64 [0/0]
    via ::, 00:15:06, vlan3
L   2001:2::1/128 [0/0]
    via ::, 00:15:05, lo0
R   2001:3::/64 [120/2]
```

```
    via fe80::201:7aff:fec3:38a4, 00:03:10, vlan2
R   2001:4::/64 [120/2]
    via fe80::201:7aff:fe11:2214, 00:03:10, vlan3
R   2001:5::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 00:03:10, 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 the receiving or advertising direction.

6.6.3.4 Configure RIPng Route Filtration

Network Requirements

Run RIPng between Device1 and Device2 for route interaction.

Device1 has learnt the two routes 2001:2::/64 and 2001:3::/64 advertised by Device2, and then, the route 2001:3::/64 is filtered in the advertising direction of Device2.

Network Topology

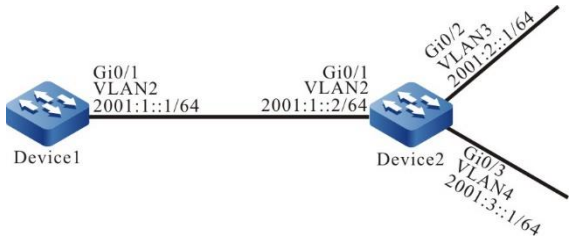


Figure 116 Networking for configuring RIPng Route filtration

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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
```

#View the IPv6 route 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:02:47:44, lo0
C   2001:1::/64 [0/0]
     via ::, 00:56:34, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:56:32, lo0
R   2001:2::/64 [120/2]
```

```
    via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
```

You can see that Device1 has learnt the two routes advertised by Device2.

Step 4: Configure the IPv6 prefix list.

```
Device2(config)#ipv6 prefix-list RIPng deny 2001:3::/64
```

Step 5: Configure the route filtration.

#Configure route filtering 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.

#View the IPv6 route 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:03:03:49, lo0
C   2001:1::/64 [0/0]
    via ::, 01:12:39, vlan2
L   2001:1::1/128 [0/0]
    via ::, 01:12:38, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:43:16, 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 the receiving or advertising direction.

6.6.3.5 Configure RIPng Route Summary

Network Requirements

Device1, Device2, Device3, and Device4 runs the RIPng protocol for the route interaction.

Device1 has learnt two routes 2001:4:1:1::/64 and 2001:4:1:2::/64 from Device2. To reduce the size of the route table, Device2 needs to advertise the summary route of the two routes to Device1.

Network Topology

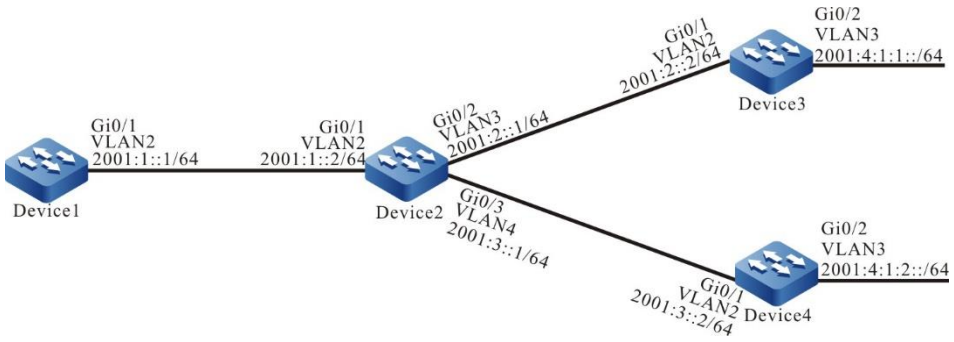


Figure - 117 Networking for configuring RIPng route summary

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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
```

#View the IPv6 route 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:02:27:40, lo0
C   2001:1::/64 [0/0]
    via ::, 00:36:29, vlan2
L   2001:1::1/128 [0/0]
    via ::, 00:36:28, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R   2001:4:1:1::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R   2001:4:1:2::/64 [120/3]
    via fe80::201:7aff:fec3:38a4, 00:06:55, vlan2
```

Step 4: Configure the route summary of the interface.

#On Device2, configure the summary route 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.

#View the IPv6 route 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:02:35:44, lo0
C   2001:1::/64 [0/0]
    via ::, 00:44:33, vlan2
L   2001:1::1/128 [0/0]
    via ::, 00:44:32, lo0
R   2001:2::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R   2001:4:1::/48 [120/3]
    via fe80::201:7aff:fec3:38a4, 00:05:19, vlan2
```

You can see that Device1 has learnt the summary route 2001:4:1::/48 advertised by Device2, but the two detailed routes can be deleted from the route table only after timeout.

6.6.3.6 Configure Passive RIPng Interface

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

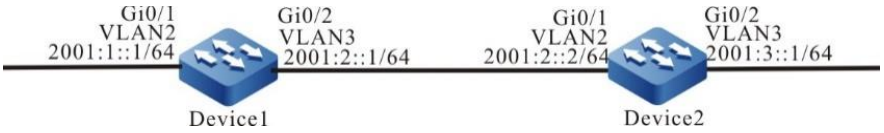


Figure-118 Networking for configuring an RIPng passive interface

Configuration Steps

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

Step 2: Configure the IPv6 address of an interface (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
```

#View the IPv6 route 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 ::, 00:21:40, lo0
C   2001:2::/64 [0/0]
     via ::, 00:21:34, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:21:33, lo0
R   2001:3::/64 [120/2]
     via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#Query the IPv6 route 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:22:39:31, lo0
R   2001:1::/64 [120/2]
     via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:30:46, vlan2
L   2001:2::2/128 [0/0]
     via ::, 00:30:45, lo0
```

```
C   2001:3::/64 [0/0]
    via ::, 00:29:12, vlan3
L   2001:3::1/128 [0/0]
    via ::, 00:29:11, 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 still can receive update packets.

Step 5: Check the result.

#View the IPv6 route 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:19:55:37, lo0
C   2001:1::/64 [0/0]
    via ::, 00:46:14, vlan2
L   2001:1::1/128 [0/0]
    via ::, 00:46:12, lo0
C   2001:2::/64 [0/0]
    via ::, 00:46:06, vlan3
L   2001:2::1/128 [0/0]
    via ::, 00:46:05, lo0
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:35:51, 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 route 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:23:05:24, lo0
C   2001:2::/64 [0/0]
    via ::, 00:56:39, vlan2
L   2001:2::2/128 [0/0]
    via ::, 00:56:38, lo0
C   2001:3::/64 [0/0]
    via ::, 00:55:05, vlan3
L   2001:3::1/128 [0/0]
    via ::, 00:55:04, lo0
```

6.6.3.7 Configure RIPng to Use IPSec Encryption Authentication

Network Requirements

Run RIPng between Device1 and Device2.

Device1 and Device2 use the IPSec tunnel to perform encryption authentication for the RIPng packets.

After configuration, the device can perform routing interaction normally.

Network Topology

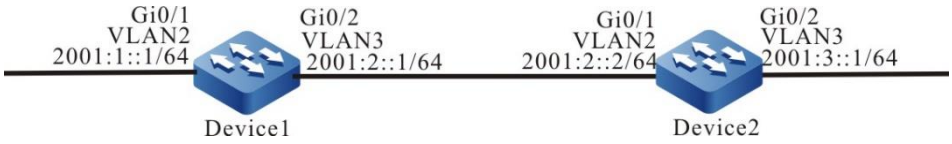


Figure 119 Networking of configuring the RIPng authentication function

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN. Configure the IPv6 address of the interface (omitted).

Step 2: Configure the RIPng process and enable the RIPng function on the interface.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
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 vlan2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

Step 3: Configure the IPSec proposal and manual tunnel.

#Configure Device1, create IPSec proposal a, adopt ESP transmission encapsulation mode, encryption algorithm 3DES, authentication algorithm sha1, create IPSec manual tunnel a, and configure 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 ipv6-tunnel a manual
Device1(config-manual-tunnel)#set ipsec proposal a
Device1(config-manual-tunnel)#set inbound esp 1000 encryption 0 11111111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaaa
Device1(config-manual-tunnel)#set outbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaaa authentication 0 1111111111111111111
Device1(config-manual-tunnel)#exit
```

#Configure Device2, create IPSec proposal a, adopt ESP transmission encapsulation mode, encryption algorithm 3des, authentication algorithm sha1, create IPSec manual tunnel a, and configure 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 ipv6-tunnel a manual
Device2(config-manual-tunnel)#set ipsec proposal a
Device2(config-manual-tunnel)#set inbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaaaa authentication 0 11111111111111111111
Device2(config-manual-tunnel)#set outbound esp 1000 encryption 0 11111111111111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaaa
Device2(config-manual-tunnel)#exit
```

Step 4: In the RIPng process, the interface is bound with the corresponding IPSec tunnel.

#On the interface vlan3 of Device1, bind the IPSec tunnel a.

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 rip ipsec-tunnel a
Device1(config-if-vlan3)#exit
```

#On the interface vlan2 of Device2, bind the IPSec tunnel a.

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 rip ipsec-tunnel a
Device2(config-if-vlan2)#exit
```

Step 5: Check the result.

#View the RIPng interface information of Device1 vlan3.

```
Device1#show ipv6 rip interface vlan3
vlan3 is up, line protocol is up
  RIPng enable status      : Enable on process 100
  RIPng running status     : Up
  VPN Routing/Forwarding   : Kernel
  Passive interface        : Disabled
  Split horizon            : enable
  Packet MTU               : 1500
  Joined RIPng multicast   : Yes
  IPv6 interface address   :
    2001:2::1/64
    fe80::201:7aff:fe74:55e7/10
  RIPng bfd interface      : Enable
  RIPng bfd function open  : OFF
```

```
RIPng bfd interface state : DOWN
RIPng ipsec-tunnel info:
  Bind to ipsec-tunnel :a
  Tunnel-id: 0
```

#View the IPv6 route 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 ::, 00:21:40, vlan2
C   2001:2::/64 [0/0]
    via ::, 00:21:34, vlan3
L   2001:2::1/128 [0/0]
    via ::, 00:21:33, vlan3
R   2001:3::/64 [120/2]
    via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#View the IPv6 route 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:22:39:31, lo0
R   2001:1::/64 [120/2]
    via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C   2001:2::/64 [0/0]
    via ::, 00:30:46, vlan2
L   2001:2::2/128 [0/0]
    via ::, 00:30:45, vlan2
C   2001:3::/64 [0/0]
    via ::, 00:29:12, vlan3
L   2001:3::1/128 [0/0]
    via ::, 00:29:11, vlan3
```

It can be seen from the routing table that the IPSec tunnel has been bound successfully, the packet sending and receiving are normal, and the route can be learned

from each other.

Note

- When configuring RIPng to bind the IPSec tunnel, you can only configure the process binding or the interface binding, and you also can configure the process and interface binding at the same time.
- When the process binding and interface binding are configured for the IPSec tunnel at the same time, the interface binding takes effect first.

6.7 OSPF

6.7.1 Overview

Open Shortest Path First (OSPF) is a dynamic routing protocol that is based on link statuses. It uses the Dijkstra's Shortest Path First (SPF) algorithm to calculate routes within a single Autonomous System (AS).

OSPF, which is developed by the Internet Engineering Task Force (IETF), solves the problems of slow convergence and liability to form loops for distance vector routes. It is applicable to medium- and large-sized networks. Currently, OSPF version 2 is available. It complies with RFC2328 and supports OSPF extended functions defined in other related RFCs.

In OSPF, each device maintains a database that describes the link status of an AS network. The databases of devices in the same area are the same. After the databases are completely synchronized, each device takes itself as the root and uses the SPF algorithm to calculate the shortest path tree without loops to describe the shortest paths it knows to reach each destination. Then each device constructs its route table based on

the shortest path tree.

The main features of OSPF include:

- Fast convergence: After the topology of the network changes, it sends an update packet immediately so that the change is synchronized in the AS.
- Loop free: OSPF runs SPF to calculate routes based on the link status database. The algorithm ensures that no routing loop will be formed.
- Dividing areas: OSPF allows to divide an AS into multiple areas to reduce network bandwidth occupancy, making it possible to construct layered network.
- Authentication support: Once an OSPF device receives a routing protocol packet, it verifies the authentication information contained in the packet to prevent information leakage or malicious attacks in the network.
- Supports subnet with different lengths: The routes advertised by OSPF carry network masks to support subnets with different lengths.
- Support load balancing: OSPF supports multiple equivalent routes to the same destination.

6.7.2 OSPF Function Configuration

Table 577 OSPF function list

Configuration Tasks	
Configure basic OSPF functions.	Enable OSPF.
Configure OSPF areas.	Configure an OSPF NSSA area.
	Configure an OSPF Stub area.
	Configure an OSPF virtual link.
	Configure the network type of an OSPF

Configuration Tasks	
Configure the OSPF network type.	interface to broadcast.
	Configure the network type of an OSPF interface to P2P.
	Configure the network type of an OSPF interface to NBMA.
	Configure the network type of an OSPF interface to P2MP.
Configure the OSPF network authentication.	Configure OSPF area authentication.
	Configure OSPF interface authentication.
Configure OSPF route generation.	Configure OSPF to redistribute routes.
	Configure the default OSPF route.
	Configure the OSPF host route.
Configure OSPF route control.	Configure route summary on inter-area OSPF routes.
	Configure OSPF external route summary.
	Configure route filtering on inter-area OSPF routes.
	Configure OSPF external route filtration.
	Configure OSPF route installation filtration.
	Configure the cost value of an OSPF interface.
	Configure the OSPF reference bandwidth.
	Configure the OSPF administrative distance.

Configuration Tasks	
	Configure the maximum number of OSPF load balancing routes.
	Configure OSPF to be compatible with RFC1583.
Configure OSPF network optimization.	Configure the keep-alive time of an OSPF neighbor.
	Configure an OSPF passive interface.
	Configure an OSPF demand circuit.
	Configure the priority of an OSPF interface.
	Configure the MTU of an OSPF interface.
	Configure the LSA transmit delay of an OSPF interface.
	Configure OSPF LSA retransmission.
	Configure OSPF to prevent LSA flooding.
	Configure OSPF SPF calculation time.
	Configure OSPF database overflow.
Configure OSPF to coordinate with BFD.	Configure OSPF to coordinate with BFD.
Configure the OSPF GR	Configure OSPF GR Restarter
	Configure OSPF GR Helper

6.7.2.1 Configure Basic OSPF Functions

Before configuring OSPF functions, you must first enable the OSPF protocol before the other functions can take effect.

Configuration Conditions

Before configuring the basic OSPF functions, 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.

Enable OSPF

To enable OSPF, you must create an OSPF process, specify the address range of the networks with which the process is associated, and specify the area to which the address range belongs. If the IP address of an interface is in the network segment of an area, the interface belongs to the area and the OSPF function is enabled, and OSPF advertises the direct route of the interface.

A device that runs OSPF must have a Router ID, which is used to uniquely identify a device in an OSPF AS. You must ensure that the Router IDs are unique in an AS; otherwise, setup of neighbors and route learning are affected. A Router ID can be specified when the OSPF process is created. If the Router ID is not specified, it can be elected according to the following rules:

- Select the biggest IP address from loopback interface IP addresses as the Router ID.
- If no loopback interface is configured with an IP address, select the biggest IP address from the IP addresses of other interfaces as the Router ID.
- Only when an interface is in the UP status can the IP address of the interface be elected as the Router ID.

OSPF supports multiple processes, which are identified by different process numbers. The processes are independent of each other, and they do not affect each other.

Table 578 Enable OSPF

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an OSPF process and enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	Mandatory. Enable the OSPF process or enable the OSPF process from VRF. By default, OSPF is disabled. If you enable OSPF from VRF, the OSPF process that belongs to a VRF can manage only interfaces under the VRF.
Configure network segments that are covered by an OSPF area.	network *ip-address wildcard-mask* area *area-id*	Mandatory. By default, an interface does not belong to any OSPF process or area. A interface can only belong to an OSPF process and area.
Configure the Router ID of the OSPF process.	router-id *ip-address*	Optional. By default, the election rule based on Router ID is generated. Modifying Router ID will not make OSPF neighbor become invalid. To make the new Router ID take effect, you need to reset the process manually.

6.7.2.2 Configure OSPF Areas

To prevent a large amount of database information from occupying too much CPU and memory, you can divide an OSPF AS into multiple areas. An area can be identified with a 32-bit area ID, a decimal number in the range of 0-4294967295, or an IP address in the range of 0.0.0.0-255.255.255.255. Area 0 or 0.0.0.0 represents an OSPF backbone area, while other non-zero areas are non-backbone areas. All routing information between areas must be forwarded through the backbone area. Non-backbone areas cannot directly exchange routing information.

OSPF defines several types of routers:

- Internal router: All interfaces belong to the devices in one area.
- Area Border Router (ABR): It is connected to devices from different areas.
- Autonomous System Boundary Router (ASBR): It is a device that introduces external routes to the OSPF AS.

Configuration Condition

Before configuring an OSPF area, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure an OSPF NSSA Area

A Not-So-Stub-Area (NSSA) does not allow injection of Type-5 Link State Advertisement (LSA) but it allows injection of Type-7 LSA. External routes can be introduced to an NSSA area through redistribution of configuration. The ASBR in the NSSA area generate Type-7 LSAs and flood LSAs to the NSSA area. The ABR in an NSSA area converts Type-7 LSAs into Type-5 LSAs, and floods the converted Type-5 LSAs into the entire AS.

The OSPF NSSA area that is configured by using the **area** *area-id* **nssa no-**

summary command is called a totally NSSA area. An OSPF totally NSSA area does not allow cross-area routes to flood in the area. At this time, the ABR generates a default route and flood it into the NSSA area. The devices in the NSSA area access a network outside the area through the default route.

Table 579 Configure an OSPF NSSA area

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure an NSSA area.	area *area-id* nssa [[default-information-originate [metric *metric-value* / metric-type *type-value*] / no-redistribution / no-summary / suppress-fa / translator-role { always | candidate | never }] | [translate-always | translate-candidate | translate-never]]	Mandatory. By default, an area is not an NSSA area.

Note

- A backbone area cannot be configured as an NSSA area.
- All devices in one NSSA area must be configured as NSSA areas, because devices with different area types cannot form neighbor relations.

Configure an OSPF Stub Area

A Stub area does not allow external route outside an AS to flood in the area so as

to reduce the size of the link status database. After an area is configured as a Stub area, the ABR which is located at the Stub border generates a default route and flood the route into the Stub area. The devices in the Stub area access a network outside the area through the default route.

The OSPF Stub area that is configured by using the **area** *area-id* **stub no-summary** command is called a totally Stub area. An OSPF totally Stub area does not allow inter-area routes and external routes to flood in the area. The devices in the area access a network outside the area and outside the OSPF AS through the default route.

Table 580 Configure an OSPF stub area

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure a Stub area.	area *area-id* stub [no-summary]	Mandatory. By default, an area is not a Stub area.
Configure the ABR in the Stub area to generate the cost value of the default route.	area *area-id* default-cost *cost-value*	Optional. By default, the ABR of the Stub area sets the cost value of the default route to 1.

Note

- A backbone area cannot be configured as a Stub area.
- All devices in one Stub area must be configured as Stub areas, because devices with different area types cannot form neighbor relations.

Configure an OSPF Virtual Link

The non-backbone areas in OSPF must synchronize and exchange data through the backbone area. Therefore, all non-backbone areas must keep connected with the backbone area.

If the requirement fails to be meet in certain cases, you can solve the problem by configuring a virtual link. After configuring a virtual link, you can configure an authentication mode for the virtual link and modify the Hello interval. The meanings of the parameters are the same as the meanings of the parameter of common OSPF interfaces.

Table -581 Configure an OSPF virtual link

Step	Command	Description
Enter the 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 [key-chain|message-digest | null] key-chain *keychain-name* | authentication-key *key* | message-digest-key *key-id* { md5 | sm3 } *key*] / dead-interval *seconds* hello-interval *seconds* / retransmit-interval *seconds* / transmit-delay *seconds*]	Mandatory. By default, no virtual link is created.

Note

- A virtual link must be configured between two ABRs.
- Two ABRs on which the virtual link is configured must be in the same public area. This area is also called the transit area of the virtual link.
- The transit area of a virtual link must not be a Stub area or NSSA area.

6.7.2.3 Configure OSPF Network Type

According to the link protocol types, OSPF classifies networks into four types:

- Broadcast Network: When the link protocol of the network is Ethernet or Fiber Distributed Data Interface (FDDI), the default OSPF network type is broadcast network.
- Point To Point Network (P2P Network): When the link protocol is Point to Point Protocol (PPP), Link Access Procedure Balanced (LAPB), or High-level Data Link Control (HDLC), the default OSPF network type is P2P network.
- Non-Broadcast Multi-Access Network (NBMA Network): When the link protocol is ATM, frame relay, or X.25, the default OSPF network type is NBMA.
- Point To Multi-Point Network (P2MP): No link protocol will be regarded by OSPF as the P2MP network by default. Usually, the NBMA network that is not totally connected is configured as the OSPF P2MP network.

You can modify the network type of an OSPF interface according to the actual requirement. The network types of the interfaces through which OSPF neighbors are set up must be the same; otherwise, normal learning of routes is affected.

Configuration Condition

Before configuring the OSPF network type, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure the Network Type of an OSPF Interface to Broadcast

A broadcast network supports multiple devices (more than two devices). These devices can exchange information with all the devices in the network. OSPF uses Hello packets to dynamically discover neighbors.

Table 582 Configure the network type of an OSPF interface to broadcast

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the network type of an OSPF interface to broadcast.	ip ospf network broadcast	Mandatory. By default, the network type of an OSPF interface is determined by the link layer protocol.

Configure the Network Type of an OSPF Interface to P2P

A P2P network is a network that consists of two devices. Each device is located at one end of a P2P link. OSPF uses Hello packets to dynamically discover neighbors.

Table 583 Configure the network type of an OSPF interface to P2P

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the OSPF network type to P2P.	ip ospf network point-to-point	Mandatory. By default, the network type of an OSPF interface is determined by the link layer protocol.

Configure the Network Type of an OSPF Interface to NBMA

An NBMA network supports multiple devices (more than two devices), but the devices does not have the broadcast capability, therefore, you must specify a neighbor manually.

Table 584 Configure the network type of an OSPF interface to NBMA

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the OSPF network type to NBMA.	ip ospf network non-broadcast	Mandatory. By default, the network type of an OSPF interface is determined by the link layer protocol.

Step	Command	Description
Enter the global configuration mode.	exit	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure a neighbor for the NBMA network.	neighbor *neighbor-ip-address* [cost *cost-value* / priority *priority-value* / poll-interval *interval-value*]	Mandatory. In an NBMA network, a neighbor must be specified manually.

Configure the Network Type of an OSPF Interface to P2MP

When an NBMA network is not fully connected, you can configure its network type to P2MP to save network overhead. If the network type is configured to P2MP unicast, you need to specify a neighbor manually.

Table 585 Configure the network type of an OSPF interface to P2MP

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the OSPF network type to P2MP.	ip ospf network point-to-multipoint [non-broadcast]	Mandatory. By default, the network type of an OSPF interface is determined by the link layer protocol.
Enter the global	exit	-

Step	Command	Description
configuration mode.		
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure a neighbor for the P2MP unicast network.	neighbor *neighbor-ip-address* [cost *cost-value* / priority *priority-value* / poll-interval *interval-value*]	If the interface network type is set to P2MP unicast, it is mandatory.

6.7.2.4 Configure OSPF Network Authentication

To prevent information leakage or malicious attacks to OSPF devices, all packet interaction between OSPF neighbors has the authentication capability. The authentication types include: NULL (no authentication), plain text authentication, MD5 authentication, and key-chain authentication.

If authentication is configured, an OSPF interface requires authentication before receiving OSPF protocol packets. The OSPF interface receives only packets that have passed authentication. Therefore, the OSPF interfaces through which neighbor relations are set up, their authentication modes, Key IDs, and authentication passwords must be the same.

An authentication mode and an authentication password are configured independently.

An OSPF authentication mode can be configured on an area, interface, or interface address. The priorities that are sorted from low to high include: area authentication, interface authentication, and interface address authentication. That is, the interface address authentication is first used, and then the interface authentication, and finally the area authentication.

Configuration Condition

Before configuring OSPF authentication, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure OSPF Area Authentication

To validate OSPF area authentication, you must configure not only the area authentication mode but also the corresponding authentication password on the interface.

Table 586 Configure OSPF area authentication

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure the area authentication mode.	area *area-id* authentication [message-digest | key-chain]	Mandatory. By default, area authentication is not configured. The keyword message-digest in the command indicates MD5 or SM3 authentication and the key word key-chain indicates the key-chain authentication. Otherwise, plain text authentication is configured.
Enter the interface	interface *interface-name*	-

Step	Command	Description
configuration mode.		
Configure a password for plain text authentication.	ip ospf [*ip-address*] authentication-key { 0 | 7 } *password*	Mandatory. By default, no password is configured for plain text authentication.
Configure a password for MD5 or SM3 authentication.	ip ospf [*ip-address*] message-digest-key *key-id* { md5 | sm3 } { 0 | 7 } *password*	Mandatory. By default, no password is configured for MD5 or SM3 authentication.
Configure the key-chain authentication	ip ospf [*ip-address*] key-chain *key-chain name*	Mandatory By default, do not configure the key-chain authentication.

Configure OSPF Interface Authentication

If an OSPF interface has multiple IP addresses, you can set an authentication mode or authentication password for one IP address of the interface. If you do not specify an interface address, all addresses of the interface use the specified authentication mode or authentication password.

Table 587 Configure OSPF interface authentication

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface interface-name	-
Configure the interface	ip ospf [ip-address] authentication	Mandatory.

Step	Command	Description
authentication mode.	[key-chain | message-digest | null]	By default, interface authentication mode is not configured. The keyword message-digest in the command indicates MD5 or SM3 authentication, the key word key-chain indicates the key-chain authentication, and the keyword null indicates no authentication; otherwise, plain text authentication is configured.
Configure a password for plain text authentication.	ip ospf [ip-address] authentication-key { 0 | 7 } password	Mandatory. By default, no password is configured for plain text authentication.
Configure a password for MD5 or SM3 authentication.	ip ospf [ip-address] message-digest-key key-id { md5 | sm3 } { 0 | 7 } password	Mandatory. By default, no password is configured for MD5 or SM3 authentication.
Configure the key-chain authentication	ip ospf [ip-address] key-chain key-chain name	Mandatory By default, do not configure the key-chain authentication.

6.7.2.5 Configure OSPF Route Generation

OSPF uses the **network** command to cover routes of the directly connected

network segment. It can also redistribute external routes or use the **host** command to add host routes.

Configuration Condition

Before configuring OSPF route generation, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure OSPF to Redistribute Routes

If multiple routing protocols run on one device, routes of other protocols can be introduced to OSPF through redistribution. By default, class 2 external routes of OSPF are generated, with the routing metric 20. When you introduces external routes through redistribution, you can modify the external route type, metric, and tag field, and configure the required routing policy to perform route control and management.

Table 588 Configure OSPF to redistribute routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF to redistribute routes.	redistribute *protocol* [*protocol-id*] [metric *metric-value* / metric-type *metric-type* / tag *tag-value* / route-map *route-map-name* / match *route-type*]	Mandatory. By default, route redistribution is not configured for OSPF.

Step	Command	Description
Configure the metric of the OSPF external routes.	default-metric *metric-value*	Optional.
Configure the limit for the number of the external routes redistributed by OSPF	redistribute maximum-prefix maximum-prefix-value [threshold-value [warning-only] / warning-only]	Optional By default, OSPF does not have the limit for the re-distributed external routes.

Note

- When configuring the commands **redistribute** *protocol* [*protocol-id*] **metric** and **default-metric** to set the metric value of the external route at the same time, the former has higher priority.

Configure the Default OSPF Route

After an OSPF Stub area or a totally NSSA areas is configured, a Type-3 default route is generated. For an NSSA area, no default route is automatically generated. You can use the **area** *area-id* **nssa default-information-originate** command to introduce a Type-7 default route to the NSSA area.

OSPF cannot use the **redistribute** command to introduce a Type-5 default route. To do this, use the **default-information originate** [**always**] command.

Table 589 Configure the default OSPF route

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

Step	Command	Description
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF to introduce a default route.	default-information originate [always / metric *metric-value* / metric-type *metric-type* / route-map *route-map-name*]	Mandatory. By default, no external default route is introduced to an OSPF AS. The default metric of the introduced default route is 1, and the type is external type 2. The field always means to force the OSPF AS to generate a default route; otherwise, the default route is generated only when there is a default route in the local route table.

Configure the OSPF Host Route

Table 590 Configure the OSPF host route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPF host route.	host *ip-address* area *area-id* [cost *cost*]	Mandatory. By default, no host route is generated.

6.7.2.6 Configure OSPF Route Control

Configuration Condition

Before configuring OSPF route control, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure Route Summary on Inter-Area OSPF Routes

When an ABR in OSPF advertises inter-area routes to other areas, it advertises each route separately in the form of Type-3 LSA. You can use the inter-area route summary function to summarize some continuous network segments to form a summary route. Then the ABR advertises the summary route, reducing the size of OSPF databases.

Table 591 Configure route summary on inter-area OSPF routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure route summary on inter-area OSPF routes.	area *area-id* range *ip-address/mask-length* [advertise [cost *cost*] | cost *cost* | not-advertise]	Mandatory. By default, an ABR does not summarize inter-area routes.

Note

- The OSPF inter-area route summary function is valid only for ABRs.
- By default, the minimum cost value among the cost values of the routes in the route summary is used as the cost value of the route summary.

Configure OSPF External Route Summary

When OSPF redistributes external routes, it advertises each route separately in the form of external LSA. You can use the external route summary function to summarize some continuous network segments to form a summary route. Then OSPF advertises the summary route, reducing the size of OSPF databases.

If you run the **summary-address** command on an ASBR, you can summarize all Type-5 LSAs and Type-7 LSAs within the address range.

Table 592 Configure OSPF external route summary

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the OSPF configuration mode.	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF to summarize external routes.	**summary-address** *ip-address mask* [**not-advertise** | **tag** *tag-value*]	Mandatory. By default, an ABR does not summarize external routes.

Note

- The OSPF external route summary function is valid only for ASBRs.

Configure Route Filtering on Inter-Area OSPF Routes

When an ABR receives inter-area routes, it performs filtration in the incoming direction based on an ACL or prefix list. When the ABR advertises inter-area routes, it performs filtration in the outgoing direction based on an ACL or prefix list.

Table 593 Configure route filtering on inter-area OSPF routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure route filtering on intra-area OSPF routes.	area *area-id* filter-list { access { *access-list-name* | *access-list-number* } | prefix *prefix-list-name* } { in | out }	Mandatory. By default, an ABR does not filter inter-area routes.

Note

- In filtration based on ACL, only a standard ACL is supported.
- The OSPF inter-area route filtering function is valid only for ABRs.

Configure OSPF External Route Filtration

Configuring OSPF external route filtering is to apply an ACL or prefix list to allow or not allow external routes of an OSPF AS to flood into the OSPF AS.

Table 594 Configure OSPF external route filtration

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

Step	Command	Description
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure a distribution list to filter external routes.	distribute-list { *access-list-name* | *access-list-number* | prefix *prefix-list-name* } out [*routing-protocol* [*process-id*]]	Mandatory. By default, an ASBR does not filter external routes.

Note

- In filtration based on ACL, only a standard ACL is supported.
- The OSPF external route filtering function is valid only for ASBRs.

Configure OSPF Route Installation Filtration

After OSPF calculates routes through LSA, to prevent certain routes from being added into the route table, OSPF filters the calculated OSPF routing information.

Three filtration methods are available:

- Filtration based on the prefix. An ACL or prefix list is used to filter the destination addresses of routes.
- Filtration based on the next hop. A prefix list is used to filter the next hops of the routes. You can also use a prefix list to filter both the destination addresses and next hops of the routes.
- Filtration of routes based on the routing policy.

Table 595 Configure OSPF route installation filtration

Step	Command	Description
Enter the global	configure terminal	-

Step	Command	Description
configuration mode.		
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF to prohibit installed routes.	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*]	Mandatory. By default, the installed routes are not filtered.

Note

- Filtration based on prefix, gateway, and route-map is mutual exclusive with filtration based on ACL. For example, if you have configured filtration based on prefix, you cannot configure filtration based on ACL again.
- Filtration based on route-map and prefix is mutual exclusive with filtration based on gateway.
- Filtration based on prefix and filtration based on gateway overwrite each other.

Configure the Cost Value of an OSPF Interface

By default, the cost of an OSPF interface is calculated based on the following formula: Reference bandwidth/Interface bandwidth.

Table 596 Configure the cost value of an OSPF interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the cost value of an OSPF interface.	ip ospf [*ip-address*] cost *cost-value*	Optional. By default, the cost value is calculated through the formula Reference bandwidth/Interface bandwidth.

Configure the OSPF Reference Bandwidth

The reference bandwidth of an interface is used to calculate the cost value of the interface. The default value is 100Mbit/s. The formula for calculating the cost value of the OSPF interface is: Reference bandwidth/Interface bandwidth. If the calculation result is larger than 1, use the integer part. If the calculation result is smaller than 1, use the value 1. Therefore, in a network whose bandwidth is larger than 100Mbit/s, the optimal route fails to be selected. In this case, you can use the **auto-cost reference-bandwidth** command to configure a proper reference bandwidth to solve the problem.

Table 597 Configure the OSPF reference bandwidth

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-

Step	Command	Description
Configuring the OSPF interface reference bandwidth.	auto-cost reference-bandwidth *reference-bandwidth*	Optional. By default, the reference bandwidth is 100Mbit/s.

Configure the OSPF Administrative Distance

An administrative distance is used to indicate the reliability of the routing protocol. If the routes to the same destination network are learnt by different routing protocols, the route with the smallest administrative distance is selected with priority.

Table 598 Configure the OSPF administrative distance

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPF administrative distance.	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 intra-area and inter-area OSPF routes is 110, and the administrative distance of external routes is 150.

Configure the Maximum Number of OSPF Load Balancing Routes

If multiple equivalent paths are available to reach the same destination, load balancing is achieved. This improves the utility rate of links and reduces the load of

the links.

Table 599 Configure the maximum number of OSPF load balancing routes

Step	Command	Description
Enter the 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 routes.	maximum-path *max-number*	Optional. By default, the maximum number of OSPF load balancing routes is 4.

Configure OSPF to Be Compatible with RFC1583

If there exist multiple paths to an ASBR or external route forwarding address, RFC1583 and RFC2328 define different routing rules. If OSPF is configured to be compatible with RFC1583, the intra-area or inter-area paths in the backbone area is selected with priority. If OSPF is configured not to be compatible with RFC1583, the intra-area paths in non-backbone networks are selected with priority.

Table 600 Configure OSPF to be compatible with RFC1583

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF to be	compatible rfc1583	Mandatory.

compatible with RFC1583.		By default, OSPF is not compatible with RFC1583.

Note

- In an OSPF AS, the routing rules of all the devices must be the same, that is, they must be all configured to be compatible with or not compatible with RFC1583 to prevent routing loops.

6.7.2.7 Configure OSPF Network Optimization

Configuration Condition

Before configuring OSPF network optimization, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure the Keep-alive Time of an OSPF Neighbor

OSPF Hello packets are used to set up neighbor relations and keep the relations alive. The default transmission interval of Hello packets is determined by the network type. For broadcast networks and P2P networks, the default transmission interval of Hello packets is 10s. For P2MP networks and NBMA networks, the default transmission interval of Hello packets is 30s.

Neighbor dead time is used to determine the validity of a neighbor. By default, the neighbor dead time is four times the Hello interval. If an OSPF device fails to receive Hello packets from a neighbor after the neighbor dead time times out, the OSPF device regards the neighbor as invalid, and then it deletes the neighbor in an active manner.

Table 601 Configure the keep-alive time of an OSPF neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure an OSPF Hello interval.	ip ospf [*ip-address*] hello-interval *interval-value*	Optional. The default value is determined by the network type. For broadcast networks and P2P networks, the default value is 10s. For P2MP networks and NBMA networks, the default value is 30s.
Configure the OSPF neighbor dead time.	ip ospf [*ip-address*] dead-interval *interval-value*	Optional. By default, the time is four times the Hello interval.

Note

- The Hello interval and neighbor dead time of OSPF neighbors must be the same; otherwise, they cannot set up neighbor relations.
- When you modify the Hello interval, if the current neighbor dead time is four times the Hello interval, the neighbor dead time is automatically modified to be still four times the new Hello interval. If the current neighbor dead time is not four times the Hello interval, the neighbor dead time keeps unchanged.

- If you modify the neighbor dead time, the Hello interval is not affected.

Configure an OSPF Passive Interface

The dynamic routing protocol adopts a passive interface to effectively decrease the network bandwidth consumed by the routing protocol. After an OSPF passive interface is configured, you can use the **network** command to advertise the routes of the directly connected network segment in which the interface is located, but the receiving and transmitting of OSPF packets are damped on the interface.

Table 602 Configure an OSPF passive interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure an OSPF passive interface.	passive-interface { *interface-name* [*ip-address*] | default }	Mandatory. By default, no OSPF passive interface is configured.

Configure an OSPF Demand Circuit

On P2P and P2MP links, to decrease the line cost, you can configure an OSPF demand circuit to suppress periodical transmitting of Hello packets and periodical update of LSA packets. This function is mainly applied on charged links such as ISDN, SVC, and X.25.

Table 603 Configure an OSPF demand circuit

Step	Command	Description
Enter the global	configure terminal	-

Step	Command	Description
configuration mode.		
Enter the interface configuration mode.	interface *interface-name*	-
Configure an OSPF demand circuit.	ip ospf [*ip-address*] demand-circuit	Mandatory. By default, no OSPF demand circuit is enabled.

Configure the Priority of an OSPF Interface

Interface priorities are mainly used in election of Designated Router (DR), and Backup Designated Router (BDR) in broadcast networks and NBMA networks. The value range is 0-255. The larger the value is, the higher the priority is. The default value is 1.

The DR and BDR are selected from all devices in a network segment based on interface priorities and Router IDs through Hello packets. The rules are as follows:

- First, the device whose interface has the highest priority is elected as the DR, and the device whose interface has the second highest priority is elected as the BDR. The device whose interface has the priority 0 does not participate in the election.
- If the interface priorities of two devices are the same, the device with the largest Router ID is elected as the DR, and the device with the second largest Router ID is elected as the BDR.
- If the DR fails, the BDR becomes the DR immediately, and a new BDR is elected.

Table 604 Configure the priority of an OSPF interface

Step	Command	Description
Enter the global	configure terminal	-

Step	Command	Description
configuration mode.		
Enter the interface configuration mode.	interface *interface-name*	-
Configure the priority of an OSPF interface.	ip ospf priority *priority-value*	Optional. By default, the OSPF interface priority is 1.

Note

- Interface priorities affect only an election process. If the DR and BDR have already been elected, modification of interface priorities does not affect the election result; instead, it affects the next election of DR or BDR. Therefore, the DR may not have the interface with the highest priority, and the BDR may not have the interface with the second highest priority.

Configure the MTU of an OSPF Interface

In encapsulating OSPF packets, to prevent fragmentation, you need to limit the packet size to equal to or smaller than Maximum Transmission Unit (MTU) of the interface. When adjacent OSPF devices exchange DD packets, MTUs are checked by default. If the MTUs are different, the devices cannot form a neighbor relation. If you have configured OSPF to ignore interface MTU check, even if MTUs are different, they can set up a neighbor relation.

Table 605 Configure the MTU of an OSPF interface

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Enter the interface configuration mode.	interface *interface-name*	-
Configure the MTU of an OSPF interface.	ip ospf mtu *mtu-value*	Optional.
Configure the OSPF interface to ignore MTU consistency check.	ip ospf [*ip-address*] mtu-ignore	Mandatory. By default, an MTU consistency check will be performed.

Configure the LSA Transmit Delay of an OSPF Interface

LSA transmit delay refers to the time it takes for an LSA to flood to other devices. The device that sends the LSA adds the interface transmit delay to the LSA aging time. By default, once the flooding LSA passes a device, the aging time is increased by 1. You can configure the LSA transmit delay according to the network conditions. The value range is 1-840. LSA transmit delay is usually configured on low-speed links.

Table 606 Configure the LSA transmit delay of an OSPF interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the LSA transmit delay of an OSPF interface.	ip ospf transmit-delay *delay-value*	Optional. By default, the LSA transmit delay is 1s.

Configure OSPF LSA Retransmission

To ensure the reliability of data exchange, OSPF adopts the acknowledgement mechanism. If an LSA floods on a device interface, the LSA is added into the retransmission list of the neighbor. If no acknowledgement message is received from the neighbor after the retransmission time times out, the LSA is retransmitted until an acknowledgement message is received.

Table 607 Configure OSPF LSA retransmission

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the interval of OSPF LSA retransmission.	ip ospf retransmit-interval *interval-value*	Optional. By default, the retransmission interval is 5s.
Enter the global configuration mode	exit	-
Enter the OSPF configuration mode	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF LSA retransmission queue scanning interval	timers lsa retransmission *scan-time*	Optional By default, the retransmission queue scanning interval is 1250ms.

Configure OSPF to Prevent LSA Flooding

In actual network applications, redundant links may be used between OSPF neighbors under some circumstances. This configuration helps to decrease flooding of OSPF update packets on redundant links.

Table 608 Configure OSPF to prevent LSA flooding

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface interface-name	-
Configure the OSPF interface to prevent LS-UPD flooding.	ip ospf database-filter all out	Mandatory. By default, the OSPF interface does not prevent LSA flooding.

Note

- Configuring OSPF to prevent LSA spreading may result in loss of some routing information.

Configure OSPF SPF Calculation Time

If the OSPF network topology changes, routes need to be re-calculated. When the network continues to change, frequent route calculation occupies a lot of system resources. You can adjust the SPF calculation time parameters to prevent frequent network changes from consuming too many system resources.

Table 609 Configure OSPF SPF calculation time

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF SPF calculation 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* indicates the initial calculation delay, *hold-time* indicates the suppression time, and *max-time* indicates the maximum waiting time between two SPF calculations. If network changes are not frequent, you can shorten the continuous route calculation interval to *delay-time*. If network changes are frequent, you can adjust the parameters, increase the suppression time to *hold-time*×2^{n-2} (n is the number of route calculation trigger times), extend the waiting time based on the configured *hold-time* increment and the maximum value must not exceed *max-time*.

Configure OSPF Database Overflow

OSPF database overflow is used to limit the number of Type-5 LSAs in the database.

Table 610 Configure OSPF Databases overflow

Step	Command	Description
Enter the global configuration mode.	**configure terminal**	-
Enter the OSPF configuration mode.	**router ospf** *process-id* [**vrf** *vrf-name*]	-
Configure OSPF database overflow.	**overflow database external** *max-number seconds*	Mandatory. By default, the OSPF database overflow function is disabled.

Caution

- After the database overflow function is enabled, the databases in the OSPF area may become inconsistent, and some routes get lost.

6.7.2.8 Configure OSPF to Coordinate with BFD

Configuration Condition

Before configuring OSPF to coordinate with BFD, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure OSPF to Coordinate with BFD

Bidirectional Forwarding Detection (BFD) provides a method for quickly detecting the status of a line between two devices. If BFD is started between two adjacent OSPF devices, if the line between two devices becomes faulty, BFD quickly detects the fault and informs OSPF of the fault. Then, it triggers OSPF to start route

calculation and switch over to the backup line, achieving fast switchover of routes.

Table 611 Configure OSPF to coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Enable or disable BFD on the specified OSPF interface.	ip ospf bfd [*ip-address* | disable]	Mandatory. By default, the BFD function is disabled.
Enter the global configuration mode.	exit	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Enable BFD on all interfaces of the OSPF process.	bfd all-interfaces	Optional.

Note

- If BFD is configured both in OSPF configuration mode and interface configuration mode, the BFD configuration on the interface has the higher priority.

6.7.2.9 Configure OSPF Fast Re-routing

Configuration Condition

Before configuring OSPF fast re-routing, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable OSPF.

Configure OSPF Fast Re-routing

In the OSPF network, if the link or device fails, the packet passing the fault point will be dropped or generate the loop and the caused traffic interruption will not recover until the protocol re-converges, which often lasts for several seconds. To reduce the traffic interruption time, you can configure the OSPF fast re-routing. Apply the route map to set the backup next hop for the matched route. Once the active link fails, the traffic passing the faulty link will switch to the standby link at once.

Table 612 Configure the OSPF fast re-routing

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPF configuration mode.	router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPF process to enable the fast re-routing function	fast-reroute route-map *route-map-name*	Mandatory By default, do not enable the OSPF fast re-routing function.
Configure the OSPF process to enable the dynamic fast re-routing function	fast-reroute loop-free-alternate [route-map *route-map-name*]	Mandatory By default, do not enable the OSPF dynamic fast re-routing function.
Configure the OSPF process to enable the pic function	pic	Mandatory After enabling the pic function, enable the auto fast

Step	Command	Description
		re-routing function. By default, do not enable the OSPF pic function.

6.7.2.10 Configure OSPF GR

GR (Graceful Restart) is used to keep the route information of the forwarding layer between the local device and the neighbor device unchanged during the active/standby switchover of the devices and the forwarding is not affected. After switching the device and running again, the protocol layer of the two devices synchronizes the route information and updates the forwarding layer so that the data forwarding is not interrupted during the device switchover.

There are two roles during GR:

- GR Restarter: The device performing the protocol graceful restarting
- GR Helper: The device assisting the protocol graceful restarting

The distributed device can serve as GR Restarter and GR Helper, while the centralized device can only serve as GR Helper, assisting Restarter to complete GR.

Configuration Condition

Before configuring OSPF GR, first complete the following task:

- Configure the interface IP address, making the neighboring node available
- Enable the OSPF protocol

Configure OSPF GR Restarter

Table 613 Configure OSPF GR Restarter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the OSPF configuration mode	router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPF GR	nsf ietf	Mandatory By default, do not enable GR function. The function takes effect and the protocol needs to support the Opaque-LSA function. By default, support the Opaque-LSA function.
Configure the OSPF GR period	nsf interval *grace-period*	Optional By default, the GR period is 95s.
Configure OSPF GR proxy	graceful-restart proxy	Optional By default, enable OSPF GR proxy. GR proxy means to prepare GR packet before switching and do not need to wait until OSPF starts after switching to send GR packet to keep OSPF neighbors alive.

Note

- The OSPF GR function can be used only in the stacking environment or dual-control environment.

Configure OSPF GR Helper

GR Helper helps Restarter to complete GR. By default, the device enables the function. The **nsf ietf helper disable** command is used to disable the GR Helper function. The **nsf ietf helper strict-lsa-checking** command is used to configure Helper to perform the strict check for LSA during GR. If finding that the LSA does not change, exit the GR Helper mode.

Table 614 Configure OSPF GR Helper

Step	Command	Description
Enter the 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, enable the Helper function and do not perform the strict check for LSA.

6.7.2.11 OSPF Monitoring and Maintaining

Table 615 OSPF monitoring and maintaining

Command	Description
clear ip ospf [*process-id*] process	Reset an OSPF process.
clear ip ospf *process-id* neighbor *neighbor-ip-address* [*neighbor-router-id*]	Reset an OSPF neighbor.

Command	Description
clear ip ospf statistics [*interface-name*]	Clear OSPF interface statistics.
clear ip ospf [*process-id*] redistribution	Re-advertises external routes.
clear ip ospf [*process-id*] route	Re-calculate OSPF routes.
show ip ospf [*process-id*]	Display the OSPF basic information.
show ip ospf [*process-id*] border-routers	Display the information about the routes that have reached the boundary devices in OSPF.
show ip ospf [*process-id*] buffers	Display the size of the OSPF packet transmitting and receiving buffer.
show ip ospf [*process-id*] database [adv-router *router-id* | 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]]	Display the information about an OSPF database.
show ip ospf interface [*interface-name* [detail]]	Display the information about an OSPF interface.
show ip ospf [*process-id*] neighbor [*neighbor-id* | all | detail [all] | interface *ip-address* [detail] | statistic]	Display the information about OSPF neighbors.
show ip ospf [*process-id*] route [*ip-address mask* | *ip-address/mask-length* | external | inter-area | intra-area | statistic]	Display the information about OSPF routes.
show ip ospf [*process-id*] virtual-links	Display the information about OSPF virtual links.

Command	Description
show ip ospf [*process-id*] sham-links	Display the information about an interface on which OSPF sham links are configured. The information include interface status, cost value, and neighbor status.

6.7.3 OSPF Typical Configuration Example

6. 7. 3. 1 Configure Basic OSPF Functions

Network Requirements

- Configure OSPF for all devices, and divide the devices into three areas: Area 0, Area 1, and Area 2. After configuration, all devices should be able to learn routes from each other.
- On a back-to-back Ethernet interface, to speed up set of OSPF neighbors, you can change the network type of the OSPF interface to P2P. Modify the network type of the interfaces in Area 2 to P2P. After the configuration, all devices can learn routes from each other.

Network Topology

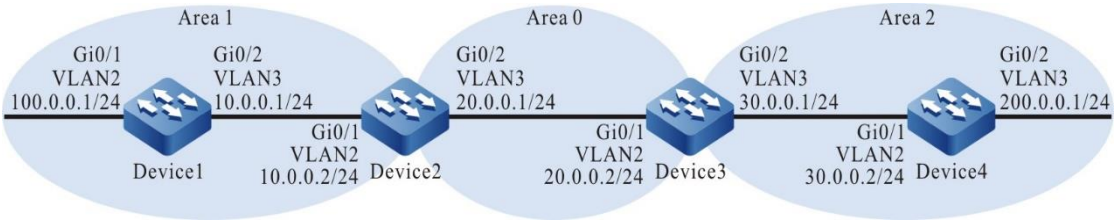


Figure 120 Networking for configuring basic OSPF functions

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process and let the interface cover different areas.

#On Device1, configure an OSPF process and configure the interfaces to cover 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
```

#On Device2, configure an OSPF process and configure the interfaces to cover Area 0 and Area 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
```

#On Device3, configure an OSPF process and configure the interfaces to cover Area 0 and Area 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
```

#On Device4, configure an OSPF process and configure the interfaces to cover 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

- A Router IDs can be manually configured or automatically generated. If a Router ID is not manually configured, the device automatically selects a Router ID. The device first selects the largest IP address among Loopback interface IP addresses as the Router ID. If the device is not configured with Loopback interface IP addresses, then it selects the largest IP addresses among common interface IP addresses as the Router ID. Only when an interface is in the UP status can the IP address of the interface be selected as the Router ID.
- In using the **network** command, the wildcard mask need not accurately match the mask length of the interface IP addresses, but the network segment needs to cover the interface IP addresses. For example, network 0.0.0.0 255.255.255.255 means to cover all interfaces.

#Query the OSPF neighbors and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

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, 02:26:23, vlan2
C   127.0.0.0/8 is directly connected, 18:09:44, lo0
O   200.0.0.0/24 [110/4] via 10.0.0.2, 02:25:36, vlan3
```

#Query the OSPF neighbors and route 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         00:00:38    20.0.0.2        vlan3

Device2#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 02:31:15, vlan2
C   20.0.0.0/24 is directly connected, 02:31:50, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 02:31:40, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 02:30:29, 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, 02:31:40, vlan3
#Query OSPF Link Status Database (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         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, routes 30.0.0.0/24 and 200.0.0.0/24 are inter-area routes. You can query the LSA information of the related routes in Summary Link States (Area 0). In the case of intra-area routes, run the **show ip ospf database router** command to query the LSA information of the related routes.

Step 4: Configure the network type of OSPF interfaces to P2P.

#On Device3, configure the OSPF network type of interface VLAN3 to P2P.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#On Device4, configure the OSPF network type of 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 neighbors and route 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     00:00:36    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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.0.0/24 [110/2] via 20.0.0.1, 00:02:53, vlan2
C   20.0.0.0/24 is directly connected, 03:20:36, vlan2
C   30.0.0.0/24 is directly connected, 03:20:26, vlan3
O   100.0.0.0/24 [110/3] via 20.0.0.1, 00:01:51, vlan2
C   127.0.0.0/8 is directly connected, 262:01:24, lo0
O   200.0.0.0/24 [110/2] via 30.0.0.2, 00:00:11, vlan3
```

Note

- If OSPF neighbor relations are set up in a P2P network, no DR or BDR election will be performed.

#Query the OSPF neighbors and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.0.0/24 [110/3] via 30.0.0.1, 00:01:04, vlan2
O   20.0.0.0/24 [110/2] via 30.0.0.1, 00:01:04, vlan2
C   30.0.0.0/24 is directly connected, 03:20:25, vlan2
O   100.0.0.0/24 [110/4] via 30.0.0.1, 00:01:04, vlan2
C   127.0.0.0/8 is directly connected, 22:52:36, lo0
C   200.0.0.0/24 is directly connected, 03:20:13, vlan3
```

After the network type of OSPF interfaces are modified to P2P, neighbors can be set up normally, and routes can be learned normally.

Note

- In configuring network types for OSPF interfaces, the network types of OSPF interfaces at the two ends of neighbors must be the same; otherwise, routing learning and flooding will be affected. By default, the network type of an OSPF interface is determined by the network type of the physical interface.

6.7.3.2 Configuring OSPF Authentication

Network Requirements

- Configure OSPF for all devices run OSPF, and configure area authentication for the devices. Configure simple text authentication for Area 0, and configure MD5 authentication for Area 1.
- Configure OSPF interface authentication, configure interface authentication of Area 0 to simple text authentication, and configure interface authentication of Area 1 to MD5 authentication.
- After configuration is completed, devices should able to normally set up neighbor relations and learn route from each other.

Network Topology

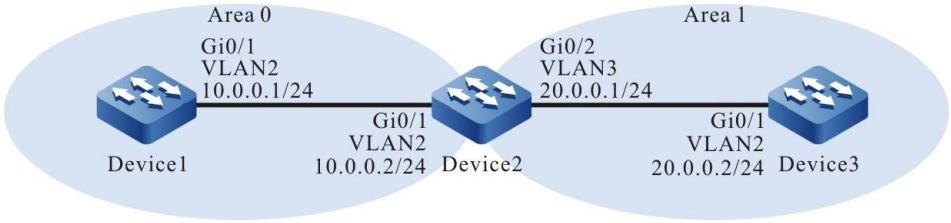


Figure 121 Networking for configuring OSPF authentication

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process, and configure the interfaces to cover different areas, and enable area authentication. Configure the simple text authentication for Area 0, and configure the MD5 authentication for Area 1.

#On Device1, configure an OSPF process and configure the 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
```

#On Device2, configure an OSPF process and configure the 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
```

#On Device3, configure an OSPF process and configure the 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
```

According to the queried information, the area authentication is the simple text mode.

#Query the OSPF neighbors and route 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         00:00:38    10.0.0.2        vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:14:01, vlan2
```

```
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:10:38, vlan2
C   127.0.0.0/8 is directly connected, 20:55:08, lo0
```

On Device1, neighbors can be normally set up, and routes can be 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 00:24:01.783 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
```

According to the queried information, the area authentication is the MD5 authentication mode.

#Query the OSPF neighbors and route 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     00:00:33    20.0.0.1        vlan2

Device3#show ip 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, E - IRMP, EX - IRMP external

O   10.0.0.0/24 [110/2] via 20.0.0.1, 00:09:31, vlan2
C   20.0.0.0/24 is directly connected, 00:20:36, vlan2
C   127.0.0.0/8 is directly connected, 24:00:06, lo0
```

On Device3, neighbors can be normally set up, and routes can be learnt normally.

Step 4: Configure OSPF interface authentication.

#On Device1, configure interface VLAN2 with simple text authentication, and set the password to 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
```

#On Device2, configure interface VLAN2 with simple text authentication, and set the password to admin. Configure interface VLAN3 with MD5 authentication, set Key ID to 1, and set password to 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
```

#On Device3, configure interface VLAN2 with MD5 authentication, set Key ID to 1, and set password to 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     00:00:33    10.0.0.1        vlan2
3.3.3.3           1   Full/DR         00:00:39    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 00:00:00
  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
```

After MD5 authentication is configured, a Crypt Sequence Number is generated.

In the case of simple text authentication, no sequence number is generated.

Note

- In configuring OSPF authentication, you can configure only area authentication or interface authentication, or configure both of them.
- If both area authentication and interface authentication are configured, interface authentication takes effect first.

6.7.3.3 Configuring OSPF to Redistribute Routes

Network Requirements

- Run OSPF between Device1 and Device2, and run RIPv2 between Device2 and Device3.
- Device2 redistributes RIP routes to OSPF, and it uses a route policy to control the device to only redistribute route 100.0.0.0/24.

Network Topology

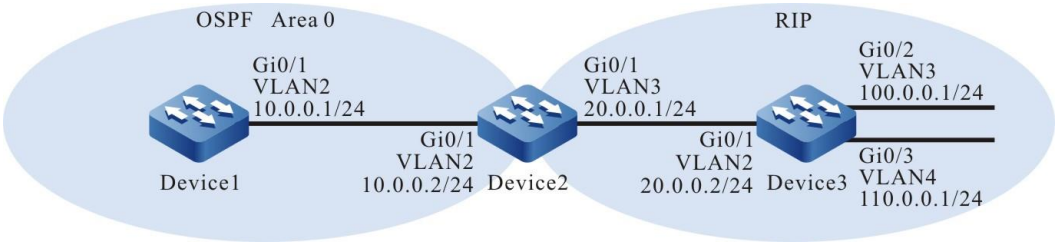


Figure 122 Networking for configuring OSPF to redistribute routes

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF between Device1 and Device2. Configure RIPv2 between Device2 and Device3.

#Configure OSPF for 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 for 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 for 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         00:00:32    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     00:00:32    10.0.0.1        vlan2
```

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:21:17, vlan2
C   20.0.0.0/24 is directly connected, 00:21:33, 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, 30:20:17, lo0
```

RIP routes have been learnt by Device2.

Step 4: Configure the routing 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
```

The route-map is configured to invoke an ACL to match only 100.0.0.0/24 while filtering out other network segment, such as 20.0.0.0/24 and 110.0.0.0/24.

Step 5: Configure OSPF to redistribute RIP routes and associate a routing policy.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map RIPtoOSPF
Device2(config-ospf)#exit
```

In redistributing RIP routes, the route-map matching rule is invoked for filtration.

Check the result.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:47:27, 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, 21:40:06, lo0
```

The route table of Device1 has learnt only the OSPF external route 100.0.0.0/24 while routes 20.0.0.0/24 and 110.0.0.0/24 have been filtered out.

#Query the OSPF process information and database 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 00:37:52.833 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]
```

According to the information about OSPF process 100, Device2 has changed its role to become an ASBR, and only one 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 redistribute routes between different routing protocols. If you really need to redistribute routes between different routing protocols, configure a routing policy to prevent routing loops.

6.7.3.4 Configure OSPF Multi-Processes

Network Requirements

- Configure OSPF on all devices. On Device2, enable two OSPF processes. Configure OSPF 100 of Device1 and that of Device2 to set up a neighbor

relation. Configure OSPF 200 of Device3 and that of Device2 to set up a neighbor relation.

- The two OSPF processes on Device2 redistribute routes to each other. OSPF process 100 uses a routing policy to control to redistribute only route 110.0.0.0/24. OSPF process 200 uses a routing policy to control to redistribute only route 100.0.0.0/24.

Network Topology

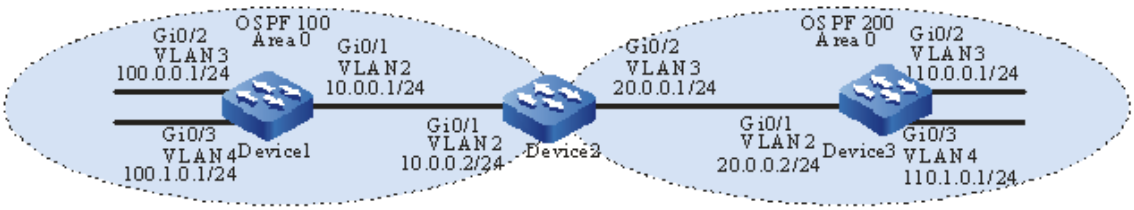


Figure 123 Networking for configuring OSPF multi-processes

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure the OSPF protocol.

#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
```

#On Device2, 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

- If there exist multiple OSPF processes, it is recommended that you configure different Router IDs for the OSPF processes to prevent Router ID conflict.

#Query the 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     00:00:30    10.0.0.1        vlan2
OSPF process 200:
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   Full/DR         00:00:33    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
```

Neighbors have been set up respectively for OSPF 100 and OSPF 200 of Device2, and the two processes have their respective OSPF databases.

#Query the OSPF route 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
```

OSPF process 100 and process 200 have calculated their own routes.

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external


C   10.0.0.0/24 is directly connected, 00:05:34, vlan2
C   20.0.0.0/24 is directly connected, 00:05:28, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2
O   100.1.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2
O   110.0.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3
O   110.1.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3
C   127.0.0.0/8 is directly connected, 48:40:33, lo0
```

Step 4: Configure the routing 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
```

The route-maps have been configured to invoke prefix list 1 and prefix list 2 to match network segment 110.0.0.0/24 and 100.0.0.0/24 respectively.

Note

- In configuring a routing 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 exactly.

Step 5: Configure OSPF processes to redistribute RIP routes to each other and associate routing policies.

#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]
```

According to the queried information, OSPF process 100 has only the LSA of external route 110.0.0.0/24, and the other routes 110.1.0.0/24 and 20.0.0.0/24 have been filtered out by the routing policy OSPF200to100. Similarly, OSPF process 200 has only the LSA of external route 100.0.0.0/24, and the other routes 100.1.0.0/24 and 10.0.0.0/24 have been filtered out by the routing policy OSPF100to200.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external


C   10.0.0.0/24 is directly connected, 00:40:20, vlan2
C   100.0.0.0/24 is directly connected, 03:11:36, vlan3
C   100.1.0.0/24 is directly connected, 01:00:22, vlan4
OE  110.0.0.0/24 [150/2] via 10.0.0.2, 00:15:27, vlan2
C   127.0.0.0/8 is directly connected, 97:08:23, lo0
```

Device1 has only learnt route 110.0.0.0/24.

#Query the route table of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external


C   20.0.0.0/24 is directly connected, 00:42:44, vlan2
OE  100.0.0.0/24 [150/2] via 20.0.0.1, 00:17:45, vlan2
C   110.0.0.0/24 is directly connected, 01:02:03, vlan3
C   110.1.0.0/24 is directly connected, 01:02:14, vlan4
C   127.0.0.0/8 is directly connected, 41:02:01, lo0
```

Device3 has only learnt route 100.0.0.0/24.

Caution

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not redistribute routes between different OSPF processes. If you really need to redistribute routes between different OSPF processes, configure a route filtering policy to prevent routing loops.

6.7.3.5 Configure OSPF External Route Summary

Network Requirements

- Run OSPF between Device1 and Device2, and run RIPv2 between Device2 and Device3.
- Device2 redistributes RIP routes to OSPF. To decrease the number of routes on Device1, summarize the redistributed RIP routes into summary route 20.0.0.0/16.

Network Topology

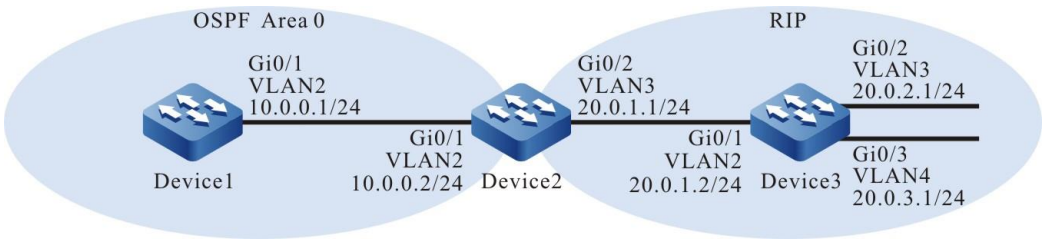


Figure 124 Networking for configuring OSPF external route summary

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: #Configure OSPF and RIPv2.

#Configure OSPF for 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 for 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 for 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 route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external


C   10.0.0.0/24 is directly connected, 00:15:46, vlan2
C   20.0.1.0/24 is directly connected, 00:15:23, vlan3
R   20.0.2.0/24 [120/1] via 20.0.1.2, 00:12:17, vlan3
R   20.0.3.0/24 [120/1] via 20.0.1.2, 00:12:06, vlan3
C   127.0.0.0/8 is directly connected, 03:34:27, lo0
```

Configure OSPF to redistribute 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]
```

According to the OSPF database, three external LSA have been generated, indicating that the RIP routes have been redistributed to OSPF.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external


C   10.0.0.0/24 is directly connected, 00:56:40, vlan2
OE  20.0.1.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
```

```
OE  20.0.2.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
OE  20.0.3.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
C   127.0.0.0/8 is directly connected, 115:12:28, lo0
```

Device1 has learnt redistributed RIP routes.

Step 5: On the ASBR, configure OSPF external route summary. Now Device2 is the ASBR.

#Configure Device2 and summarize the redistributed RIP routes into 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]
```

Comparing the result with the result in Step 3, you will find that the three external LSAs have been deleted, and a summarized external LSA has been generated.

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external
C   10.0.0.0/24 is directly connected, 00:28:03, 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, 00:27:40, vlan3
R   20.0.2.0/24 [120/1] via 20.0.1.2, 00:24:34, vlan3
R   20.0.3.0/24 [120/1] via 20.0.1.2, 00:24:23, vlan3
C   127.0.0.0/8 is directly connected, 03:46:44, lo0
```

Note

- In the route table of Device2, a summary route 20.0.0.0/16 with the output interface being Null0 has been automatically added. This route helps to prevent routing loops.

```
#Query the route table of Device1.
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.0.0.0/24 is directly connected, 00:58:40, vlan2
OE  20.0.0.0/16 [150/20] via 10.0.0.2, 00:15:26, vlan2
C   127.0.0.0/8 is directly connected, 115:17:28, lo0
```

The route table of Device1 has only learnt the summary route 20.0.0.0/16.

6.7.3.6 Configure Route Summary on Inter-Area OSPF Routes

Network Requirements

- Configure OSPF for all devices, and divide the devices into two areas, Area 0 and Area 1.
- To decrease the number of inter-area routes, inter-area routes are summarized on the ABR. The routes in Area 0 are summarized to form 10.0.0.0/16. The routes in Area 1 are summarized to form 20.0.0.0/16.

Network Topology

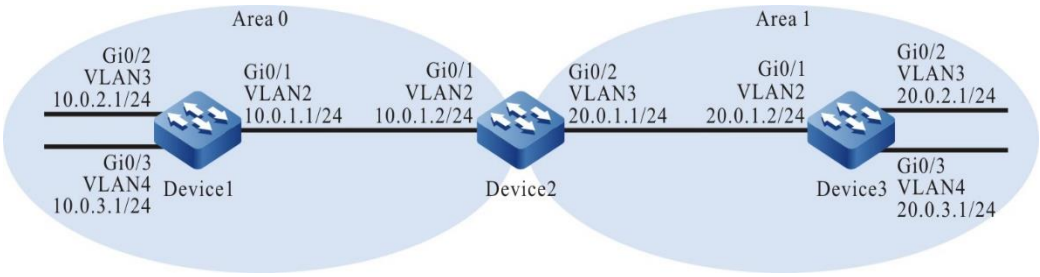


Figure 125 Networking for configuring route summary on inter-area OSPF routes

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process and let the interface cover 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 the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.0.1.0/24 is directly connected, 00:30:31, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
C   20.0.1.0/24 is directly connected, 02:09:10, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
C   127.0.0.0/8 is directly connected, 05:28:14, lo0
```

In the OSPF database of Device2, three inter-area LSAs are generated respectively for Area 0 and Area 1. The intra-area routes of the areas have also been added into the route table.

#Query the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external
```

```
C   10.0.1.0/24 is directly connected, 00:25:11, vlan2
C   10.0.2.0/24 is directly connected, 00:24:58, vlan3
C   10.0.3.0/24 is directly connected, 00:24:44, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 00:14:59, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
O   20.0.3.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
C   127.0.0.0/8 is directly connected, 116:19:42, lo0
```

The OSPF database of Device1 contains three inter-area LSAs, and the three routes have been added into the route table.

#Query the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.1.0/24 [110/2] via 20.0.1.1, 00:24:04, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
O   10.0.3.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
C   20.0.1.0/24 is directly connected, 02:09:51, vlan2
C   20.0.2.0/24 is directly connected, 02:07:21, vlan3
```

```
C   20.0.3.0/24 is directly connected, 02:07:09, vlan4
C   127.0.0.0/8 is directly connected, 360:20:45, lo0
```

Similarly, the OSPF database of Device3 contains three inter-area LSAs, and the three routes have been added into the route table.

Step 4: On the ABR, configure inter-area route summary. Now Device2 is the ABR.

#On Device2, summarize the routes in Area 0 to form route 10.0.0.0/16, and summarize the routes in Area 1 to form route 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 the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   10.0.0.0/16 [110/1] is directly connected, 00:00:31, null0
C   10.0.1.0/24 is directly connected, 00:40:31, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O   20.0.0.0/16 [110/1] is directly connected, 00:00:27, null0
C   20.0.1.0/24 is directly connected, 02:19:10, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
C   127.0.0.0/8 is directly connected, 05:38:14, lo0
```

Comparing the result with the result of Step 2, you will find that only one summarized inter-area LSA is generated respectively for Area 0 and Area 1 in the OSPF database of Device2. Similarly, a summary route with the output interface being Null0 is automatically added into the route table.

#Query the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.0.1.0/24 is directly connected, 00:40:11, vlan2
C   10.0.2.0/24 is directly connected, 00:39:58, vlan3
C   10.0.3.0/24 is directly connected, 00:39:44, vlan4
O   20.0.0.0/16 [110/2] via 10.0.1.2, 00:02:18, vlan2
C   127.0.0.0/8 is directly connected, 116:44:42, lo0
```

On Device1, you will find that the OSPF database contains only the summarized inter-area LSA, and the route table leans only the summary route 20.0.0.0/16 of Area 1. Similarly, Device3 learns only the summary route 10.0.0.0/16 of Area 0.

6.7.3.7 Configure Route Filtering on Inter-Area OSPF Routes

Network Requirements

- Configure OSPF for all devices, and divide the devices into two areas, Area 0 and Area 1.
- On the ABR, configure inter-area route filtration. According to route filtration, Area 0 does not allow injection of route 20.0.3.0/24, and 10.0.3.0/24 is not allowed to flood into other areas.

Network Topology

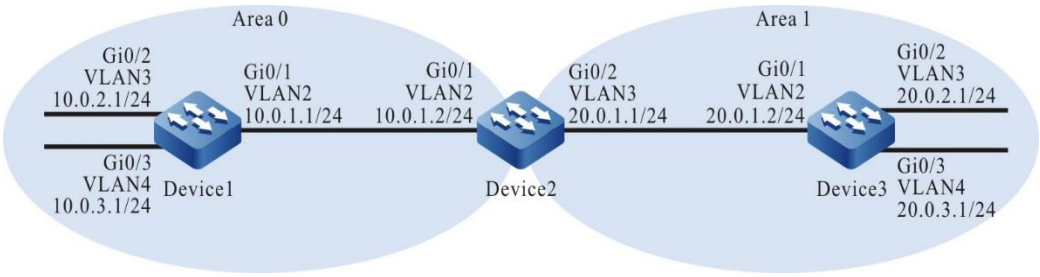


Figure 126 Networking for configuring route filtering on inter-area OSPF routes

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process and let the interface cover 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 the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


C   10.0.1.0/24 is directly connected, 00:06:13, vlan2
O   10.0.2.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
O   10.0.3.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
C   20.0.1.0/24 is directly connected, 00:06:19, vlan3
O   20.0.2.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
O   20.0.3.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
C   127.0.0.0/8 is directly connected, 94:42:22, lo0
```

In the OSPF database of Device2, three inter-area LSAs are generated respectively for Area 0 and Area 1. The intra-area routes of the areas have also been added into the route table.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external


C   10.0.1.0/24 is directly connected, 00:08:41, vlan2
C   10.0.2.0/24 is directly connected, 37:59:10, vlan3
C   10.0.3.0/24 is directly connected, 38:05:36, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 00:07:55, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 00:07:55, vlan2
O   20.0.3.0/24 [110/3] via 10.0.1.2, 00:06:50, vlan2
C   127.0.0.0/8 is directly connected, 70:07:32, lo0
```

Device1 has learnt routes of Area 1.

#Query the route table of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external


O   10.0.1.0/24 [110/2] via 20.0.1.1, 00:08:44, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 00:08:33, vlan2
O   10.0.3.0/24 [110/3] via 20.0.1.1, 00:07:30, vlan2
C   20.0.1.0/24 is directly connected, 00:09:31, vlan2
C   20.0.2.0/24 is directly connected, 37:59:57, vlan3
```

```
C   20.0.3.0/24 is directly connected, 38:03:35, vlan4
C   127.0.0.0/8 is directly connected, 61:26:38, lo0
```

Device3 has learnt routes of Area 0.

Step 4: Configure a route filtering 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 list 1 filters out network 10.0.3.0/24 and allows all other networks. Prefix list 2 filters out network 20.0.3.0/24 and allows all other networks.

Step 5: On the ABR, configure filtration of inter-area routes and invoke the matching rules of a 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
```

Comparing the result with the result of Step 2, the LSA of network 20.0.3.0/24 has been deleted from Area 0 in the OSPF database. Similarly, the LSA of network 10.0.3.0/24 has been deleted from Area 1.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.0.1.0/24 is directly connected, 00:12:57, vlan2
C   10.0.2.0/24 is directly connected, 38:03:25, vlan3
C   10.0.3.0/24 is directly connected, 38:09:52, vlan4
O   20.0.1.0/24 [110/2] via 10.0.1.2, 00:12:11, vlan2
O   20.0.2.0/24 [110/3] via 10.0.1.2, 00:12:11, vlan2
C   127.0.0.0/8 is directly connected, 70:11:48, lo0
```

The route 20.0.3.0/24 does not exist in the route table of Device1.

#Query the route table of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external

O   10.0.1.0/24 [110/2] via 20.0.1.1, 00:13:09, vlan2
O   10.0.2.0/24 [110/3] via 20.0.1.1, 00:12:58, vlan2
C   20.0.1.0/24 is directly connected, 00:13:56, vlan2
C   20.0.2.0/24 is directly connected, 38:04:22, vlan3
C   20.0.3.0/24 is directly connected, 38:08:00, vlan4
C   127.0.0.0/8 is directly connected, 64:31:03, lo0
```

The route 10.0.3.0/24 does not exist in the route table of Device3.

6. 7. 3. 8 Configure OSPF Totally Stub Area

Network Requirements

- Configure OSPF for all devices, and divide the devices into three areas: Area 0, Area 1, and Area 2. Configure Area 1 as a totally Stub area.
- On Device4, redistribute a static route to OSPF. After the configuration is completed, the totally Stub area cannot learn inter-area routes and external routes, while the devices of other areas can learn inter-area routes and external routes.

Network Topology

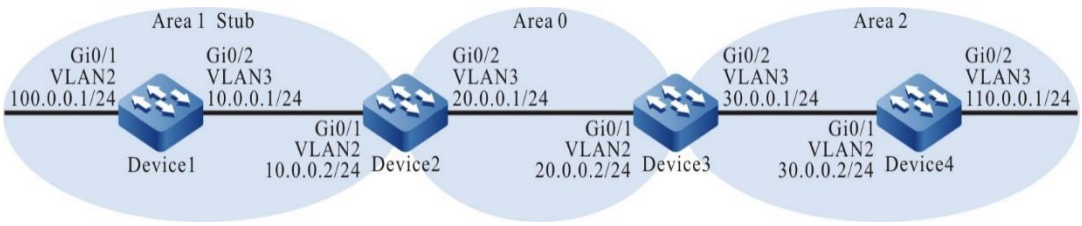


Figure 127 Networking for configuring an OSPF totally stub area

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN

(omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process and let the interfaces cover the related areas.

#Configure Device1. Configure Area 1 to a Stub area.

```
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. Configure Area 1 to a totally Stub area. Devce2 is an ABR, and the **no-summary** command takes effect only on an 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 20.0.0.0 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 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: On Device4, configure a static route, and redistribute the route into the 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 the OSPF LSDB and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
     U - Per-user Static route
     O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

O   0.0.0.0/0 [110/2] via 10.0.0.2, 00:00:19, vlan3
C   10.0.0.0/24 is directly connected, 00:01:04, vlan3
C   100.0.0.0/24 is directly connected, 00:11:55, vlan2
C   127.0.0.0/8 is directly connected, 30:46:57, lo0
```

According to the information in the OSPF database, only Area 1 has an LSA for

inter-area route 0.0.0.0/0, while the other areas do not have LSAs for inter-area or external routes. The ABR in the Stub area generates an inter-area route 0.0.0.0/0, which floods in the totally Stub area. Data is forwarded to outside of the area or AS through the default route.

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:01:02, vlan2
C   20.0.0.0/24 is directly connected, 00:00:59, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:00:17, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 00:00:10, vlan2
O   110.0.0.0/24 [110/3] via 20.0.0.2, 00:00:17, vlan3
C   127.0.0.0/8 is directly connected, 56:07:04, lo0
OE  200.1.1.0/24 [150/20] via 20.0.0.2, 00:00:16, vlan3
```

According to the queried information, you will find that Device2 is able to learn inter-area and external routes.

Note

- If you run the **area** *area-id* **stub** command but do not run the **no-summary** command, the device in the area can learn inter-area routes but cannot learn external routes. Access to a network outside the AS is still conducted through the default route.

6.7.3.9 Configure OSPF NSSA Area

Network Requirements

- Configure OSPF for all devices, and divide the devices into three areas: Area 0, Area 1, and Area 2. Configure Area 1 and Area 2 as NSSA areas.

- On Device4, redistribute a static route to OSPF. After the configuration is completed, all devices can learn intra-area and inter-area routes, but external routes cannot be injected into Area 1.
- Introduce a default route to the ABR of Area 1 so that Device1 can access an external network through the default route.

Network Topology

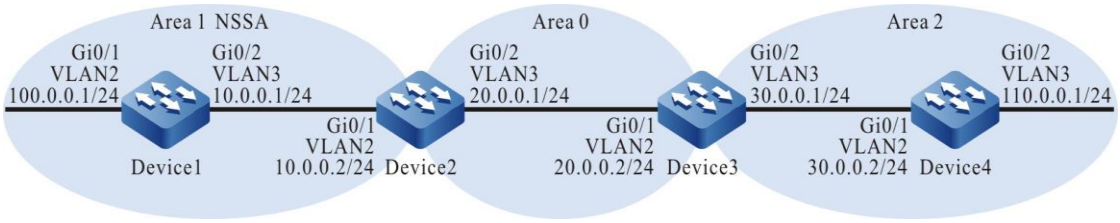


Figure 128 Networking for configuring an OSPF NSSA area

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an OSPF process and let the interfaces cover the related areas.

#Configure Device1. Configure Area 1 to an 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. Configure Area 1 to an 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 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3. Configure Area 2 to an 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. Configure Area 2 to an 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: On Device4, configure a static route, and redistribute the route into the 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]

According to the OSPF database, the ABR in the NSSA area (Area 2) converts NSSA-external LSAs into AS External LSAs. Therefore, the other areas can normally learn external routes that are redistributed from the NSSA area (Area 2).

#Query the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:02:53, vlan2
C   20.0.0.0/24 is directly connected, 00:02:51, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:04, vlan3
O   100.0.0.0/24 [110/2] via 10.0.0.1, 00:02:04, vlan2
O   110.0.0.0/24 [110/3] via 20.0.0.2, 00:02:02, vlan3
C   127.0.0.0/8 is directly connected, 06:47:22, lo0
OE  200.1.1.0/24 [150/20] via 20.0.0.2, 00:02:02, vlan3
```

Device2 has learnt the external routes that have been redistributed from the NSSA area (Area 2).

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:02:29, vlan3
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:01:44, vlan3
O   30.0.0.0/24 [110/3] via 10.0.0.2, 00:01:41, vlan3
C   100.0.0.0/24 is directly connected, 01:53:00, vlan2
O   110.0.0.0/24 [110/4] via 10.0.0.2, 00:01:40, vlan3
C   127.0.0.0/8 is directly connected, 383:45:55, lo0
```

According to the queried information, route 200.1.1.0/24 does not exist in the route table of Device1, indicating that the external route redistributed by Device4 has not been injected to the NSSA area (Area 1), while the routes of other areas have been added into the route table.

Step 5: Configure Device2, and introduce a default route to Area 1.

#Configure Device2. At this time, Device2 is the 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 **area** *area-id* **nssa no-summary** command is executed on the ABR of the NSSA area, the area is called a totally NSSA area. At this time, the ABR generates a default route and flood the default route into the NSSA area. After the command is configured, the number of summary LSAs and corresponding inter-area routes will be further decreased. The devices in the area access a network outside the area or outside the AS through the 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 has generated a NSSA-external LSA for the default route.

#Query the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external


OE  0.0.0.0/0 [150/1] via 10.0.0.2, 00:00:22, vlan3
C   10.0.0.0/24 is directly connected, 00:07:29, vlan3
O   20.0.0.0/24 [110/2] via 10.0.0.2, 00:06:44, vlan3
O   30.0.0.0/24 [110/3] via 10.0.0.2, 00:06:41, vlan3
C   100.0.0.0/24 is directly connected, 01:58:00, vlan2
O   110.0.0.0/24 [110/4] via 10.0.0.2, 00:06:40, vlan3
C   127.0.0.0/8 is directly connected, 383:50:55, lo0
```

The route table of Device1 has learnt the default route 0.0.0.0, and Device1 communicates with the network outside the AS through the default route.

6.7.3.10 Configure OSPF to Coordinate with BFD

Network Requirements

- Configure OSPF for all devices.
- Enable the BFD detection function on the line between Device1 and Device3. If the line becomes faulty, BFD quickly detects the fault and notify OSPF of the fault. Then, OSPF switches the route to Device2 for communication.

Network Topology

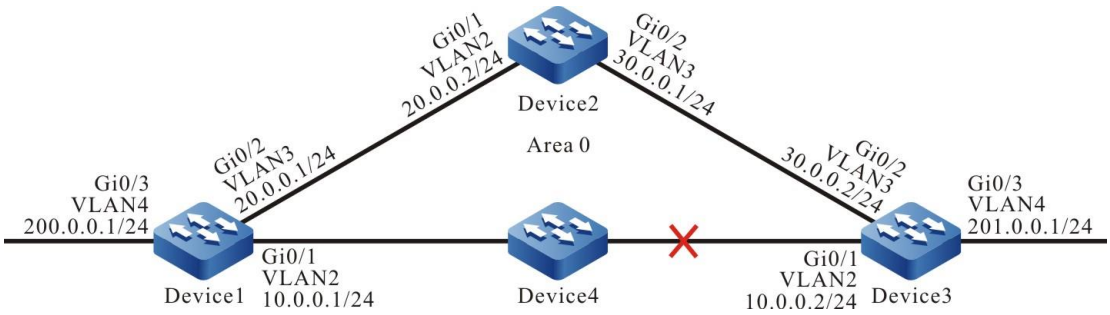


Figure 129 Networking for configuring OSPF to coordinate with BFD

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure an 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 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
```

Step 5: Check the result.

#Query the OSPF neighbors and route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:01:09, vlan2
C   20.0.0.0/24 is directly connected, 00:55:37, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:50, vlan3
                [110/2] via 10.0.0.2, 00:01:30, vlan2
C   127.0.0.0/8 is directly connected, 05:51:09, lo0
C   200.0.0.0/24 is directly connected, 00:55:12, vlan4
O   201.0.0.0/24 [110/2] via 10.0.0.2, 00:01:30, vlan2
```

According to the OSPF neighbor information, BFD has been enabled, and route

201.0.0.0/24 selects the line between Device1 and Device3 with priority 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
```

According to the queried information, OSPF has been configured successfully to coordinate with BFD, and the session has been normally set up.

#If the line between Device1 and Device3 becomes faulty, BFD quickly detects the fault and informs OSPF of the fault. OSPF then switch the route to Device2 for communication. Query the route 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, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external


C   10.0.0.0/24 is directly connected, 00:01:59, vlan2
C   20.0.0.0/24 is directly connected, 00:56:13, vlan3
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:03:40, vlan3
C   127.0.0.0/8 is directly connected, 05:52:41, lo0
C   200.0.0.0/24 is directly connected, 00:56:02, vlan4
O   201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:06, vlan3
```

The action of Device3 is similar to that of Device1.

6.7.3.11 Configure OSPF Fast Re-routing

Network Requirements

- All devices configure the OSPF protocol.

- Device1 learns the OSPF route 192.168.1.1/32 from Device2 and Device3 at the same time. Device1 first uses the line with Device3 to forward the packet. Similarly, Device3 learns the OSPF route 100.1.1.1/32 from Device1 and Device2 at the same time. Device3 first uses the line with Device1 to forward the packet.
- Device1 and Device3 enable the OSPF fast re-routing. After the line between Device1 and Device3 fails, the service can switch to Device2 for communication fast.

Network Topology

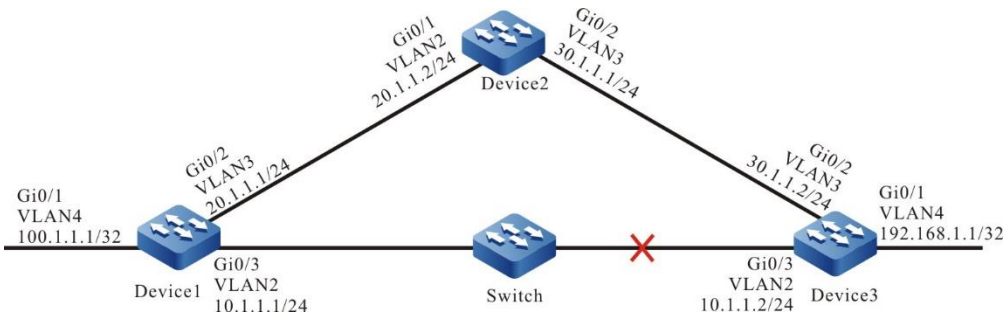


Figure 130 Configure the OSPF fast re-routing

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN; configure the IP addresses of the interfaces. (Omitted)

Step 2: Configure OSPF.

#Configure Device1. Configure the OSPF process and make the interface cover area 0.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.1.1 0.0.0.0 area 0
```

```
Device1(config-ospf)#exit
```

#Configure Device2. Configure the OSPF process and make the interface cover area 0.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3. Configure the OSPF process and make the interface cover area 0.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 192.168.1.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

Step 3: Configure the routing policy.

#Configure Device1: configure route-map to call the ACL only matching 192.168.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface vlan3 and the next-hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfrr_ospf
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#Configure Device3: configure route-map to call the ACL only matching 100.1.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface vlan3 and the next-hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
```

```
Device3(config)#route-map ipfrr_ospf
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure the fast re-routing.

#Configure Device1 to enable the OSPF fast re-routing.

```
Device1(config)#router ospf 100
Device1(config-ospf)#ipfrr route-map ipfrr_ospf
Device1(config-ospf)#exit
```

#Configure Device3 to enable the OSPF fast re-routing

```
Device3(config)#router ospf 100
Device3(config-ospf)#ipfrr route-map ipfrr_ospf
Device3(config-ospf)#exit
```

Step 5: Check the result.

#View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 00:22:44, vlan2
L   10.1.1.1/32 is directly connected, 00:22:44, vlan2
C   20.1.1.0/24 is directly connected, 06:39:56, vlan3
L   20.1.1.1/32 is directly connected, 06:39:56, vlan3
O   30.1.1.0/24 [110/2] via 20.1.1.2, 00:01:51, vlan3
                [110/2] via 10.1.1.2, 00:00:16, vlan2
C   127.0.0.0/8 is directly connected, 31:14:38, lo0
L   127.0.0.1/32 is directly connected, 31:14:38, lo0
LC   100.1.1.1/32 is directly connected, 03:14:47, vlan4
O   192.168.1.1/32 [110/2] via 10.1.1.2, 00:00:04, vlan2
```

#View the fast re-route table of Device1 and you can see that there is the route of the network 192.168.1.1/32 and the next-hop interface is vlan3.

```
Device1#show ip frr 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, E - IRMP, EX - IRMP external
```

```
O   192.168.1.1/32 [110/0] via 20.1.1.2, 00:00:08, vlan3
```

#View the backup next-hop information of Device1 and the fast re-routing backup interface is vlan3.

```
Device1#show nexthop frr detail
Index               : 225
Type                : FRR
Reference Count     : 1
Active Path         : master
Nexthop Address     : 10.1.1.2
Interface           : vlan2
Interface Vrf       : global
Channel ID          : 10
Link Header Length  : 18
Link Header         : 01017a12345320120101010181000000010800
Action              : FORWORDING
Slot                : 0
BK Nexthop Address  : 20.1.1.2
BK Interface        : vlan3
BK Interface Vrf    : global
BK Channel ID       : 11
BK Link Header Length  : 18
BK Link Header      : 01017a45544920120101010281000000020800
BK Action           : FORWORDING
BK Slot             : 0

Total 1 entries.
```

#After the line between Device1 and Device3 fails, the system can fast detect and switch to Device2 for communication. View the route table and fast re-route table of Device1. The egress interface to the destination network 192.168.1.1/32 in the route table is switched to the backup interface vlan3.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 00:22:44, vlan2
L   10.1.1.1/32 is directly connected, 00:22:44, vlan2
C   20.1.1.0/24 is directly connected, 06:39:56, vlan3
L   20.1.1.1/32 is directly connected, 06:39:56, vlan3
O   30.1.1.0/24 [110/2] via 20.1.1.2, 00:01:51, vlan3
```

```
                [110/2] via 10.1.1.2, 00:00:16, vlan2
C   127.0.0.0/8 is directly connected, 31:14:38, lo0
L   127.0.0.1/32 is directly connected, 31:14:38, lo0
LC  100.1.1.1/32 is directly connected, 03:14:47, vlan4
O   192.168.1.1/32 [110/3] via 20.1.1.2, 00:00:04, vlan3
```

The processing mode of Device3 is similar with Device1.

6.8 OSPFv3

6.8.1 Overview

OSPFv3 is the abbreviation of OSPF (Open Shortest Path First) Version 3. It mainly provides support for IPv6, follows RFC2328, RFC2740, and supports OSPF extensions defined by other related RFCs.

OSPFv3 is basically the same as OSPFv2, but there are some corresponding modifications for different IP protocols and address families. Their differences are mainly manifested in:

OSPFv3 runs based on the link, and OSPFv2 runs based on the segment

Each OSPFv3 link supports multiple instances

OSPFv3 identifies the neighbor via Router ID, and OSPFv2 identifies the neighbor via the IP address.

6.8.2 OSPFv3 Function Configuration

Table 616 OSPFv3 function list

Configuration Tasks	
Configure basic OSPFv3 functions.	Enable OSPFv3.
Configure OSPFv3 areas.	Configure an OSPFv3 NSSA area.
	Configure an OSPFv3 Stub area.
	Configure an OSPFv3 virtual link.
	Configure the network type of an OSPFv3

Configuration Tasks	
Configure the OSPFv3 network type.	interface to broadcast.
	Configure the network type of an OSPFv3 interface to P2P.
	Configure the network type of an OSPFv3 interface to NBMA.
	Configure the network type of an OSPFv3 interface to P2MP.
Configure the OSPFv3 network authentication.	Configure OSPFv3 area authentication.
	Configure OSPFv3 interface authentication.
Configure OSPFv3 route generation.	Configure OSPFv3 to redistribute routes.
	Configure the default OSPFv3 route.
Configure OSPFv3 route control.	Configure route summary on inter-area OSPFv3 routes.
	Configure OSPFv3 external route summary.
	Configure route filtering on inter-area OSPFv3 routes.
	Configure OSPFv3 external route filtration.
	Configure OSPFv3 route installation filtration.
	Configure the cost value of an OSPFv3 interface.
	Configure the OSPFv3 reference bandwidth.
	Configure the OSPFv3 administrative distance.

Configuration Tasks	
	Configure the maximum number of OSPFv3 load balancing routes.
Configure OSPFv3 network optimization.	Configure the keep-alive time of an OSPFv3 neighbor.
	Configure an OSPFv3 passive interface.
	Configure an OSPFv3 demand circuit.
	Configure the priority of an OSPFv3 interface.
	Configure the MTU of an OSPFv3 interface.
	Configure the LSA transmit delay of an OSPFv3 interface.
	Configure OSPFv3 LSA retransmission.
	Configure OSPFv3 SPF calculation time.
Configure OSPFv3 GR	Configure OSPFv3 GR Restarter
	Configure OSPFv3 GR Helper
Configure OSPFv3 to coordinate with BFD.	Configure OSPFv3 to coordinate with BFD.

6.8.2.1 Configure Basic OSPFv3 Functions

Before configuring OSPFv3 functions, you must first enable the OSPFv3 protocol before the other functions can take effect.

Configuration Conditions

Before configuring the basic OSPFv3 functions, ensure that:

- The link layer protocol has been configured to ensure normal communication at the link layer.

- Enable the IPv6 forwarding functions

Enable OSPFv3

To enable OSPFv3, you must create an OSPFv3 process, specify the Router ID of the process, and enable the OSPFv3 protocol on the interface.

A device that runs the OSPFv3 protocol must have a Router ID, which is used to uniquely identify a device in an OSPFv3 AS. You must ensure that the Router ID is unique in an AS; otherwise, setup of neighbors and route learning are affected. In OSPFv3, you need to manually configure one Router ID of the IPv4 address format.

OSPFv3 supports multiple processes, and uses the process number to identify one process. Different processes are independent of each other and have no influence on each other.

Table 617 Enable the OSPFv3 protocol

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Create an OSPFv3 process and enter the OSPF configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	Mandatory. Enable the OSPFv3 process or enable the OSPF process from VRF. By default, the OSPFv3 protocol is disabled. If you enable OSPFv3 from VRF, the OSPFv3 process that belongs to a VRF can manage only interfaces under the VRF.
Configure the Router ID of the OSPFv3 process.	router-id *ipv4-address*	Mandatory
Return to the global	exit	-

Step	Command	Description
configuration mode		
Enter the interface configuration mode	interface *interface-name*	-
Configure enabling the OSPFv3 protocol on the interface	ipv6 router ospf *process-id* area *area-id* [instance-id *instance-id*]	Mandatory By default, the OPSFv3 protocol is disabled on the interface.

6.8.2.2 Configure the OSPFv3 Area

To prevent a large amount of database information from occupying too much CPU and memory, you can divide an OSPFv3 AS into multiple areas. An area can be identified with a 32-bit area ID, a decimal number in the range of 0-4294967295, or an IP address in the range of 0.0.0.0-255.255.255.255. Area 0 or 0.0.0.0 represents an OSPFv3 backbone area, while other non-zero areas are non-backbone areas. All routing information between areas must be forwarded through the backbone area. Non-backbone areas cannot directly exchange routing information.

OSPFv3 defines several types of routers:

- Internal router: All interfaces belong to the devices in one area.
- Area Border Router (ABR): It is connected to devices from different areas.
- Autonomous System Boundary Router (ASBR): It is a device that introduces external routes to the OSPFv3 AS.

Configuration Condition

Before configuring an OSPFv3 area, ensure that:

- Enable the IPv6 forwarding function
- Enable the OSPFv3 protocol

Configure an OSPFv3 NSSA Area

A Not-So-Stub-Area (NSSA) does not allow injection of Type-5 Link State Advertisement (LSA) but it allows injection of Type-7 LSA. External routes can be introduced to an NSSA area through redistribution of configuration. The ASBR in the NSSA area generate Type-7 LSAs and flood LSAs to the NSSA area. The ABR in an NSSA area converts Type-7 LSAs into Type-5 LSAs, and floods the converted Type-5 LSAs into the entire AS.

The OSPFv3 NSSA area that is configured by using the **area** *area-id* **nssa no-summary** command is called a totally NSSA area. An OSPFv3 totally NSSA area does not allow cross-area routes to flood in the area. At this time, the ABR generates a default route and flood it into the NSSA area. The devices in the NSSA area access a network outside the area through the default route.

Table 618 Configure an OSPFv3 NSSA area

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure an NSSA area.	area *area-id* nssa [no-redistribution / no-summary / default-information-originate [metric *metric-value* / metric-type *type-value*]]	Mandatory By default, an OSPFv3 area is not the NSSA area.

Note

- A backbone area cannot be configured as an NSSA area.
- All devices in one NSSA area must be configured as NSSA areas, because devices with different area types cannot form neighbor relations.

Configure an OSPFv3 Stub Area

A Stub area does not allow external route outside an AS to flood in the area so as to reduce the size of the link status database. After an area is configured as a Stub area, the ABR which is located at the Stub border generates a default route and flood the route into the Stub area. The devices in the Stub area access a network outside the area through the default route.

The OSPFv3 Stub area that is configured by using the **area** *area-id* **stub no-summary** command is called a totally Stub area. An OSPFv3 totally Stub area does not allow inter-area routes and external routes to flood in the area. The devices in the area access a network outside the area and outside the OSPFv3 AS through the default route.

Table 619 Configure an OSPFv3 Stub area

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure a Stub area.	area *area-id* stub [no-summary]	Mandatory By default, an OSPFv3 area is not the Stub area.

Note

- A backbone area cannot be configured as a Stub area.
- All devices in one Stub area must be configured as Stub areas, because devices with different area types cannot form neighbor relations.

Configure an OSPFv3 Virtual Link

The non-backbone areas in OSPFv3 must synchronize and exchange data through the backbone area. Therefore, all non-backbone areas must keep connected with the backbone area.

If the requirement fails to be meet in certain cases, you can solve the problem by configuring a virtual link. After configuring a virtual link, you can configure an authentication mode for the virtual link and modify the Hello interval. The meanings of the parameters are the same as the meanings of the parameter of common OSPFv3 interfaces.

Table 620 Configure an OSPFv3 virtual link

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure an OSPFv3 virtual link.	area *transit-area-id* virtual-link *neighbor-id* [dead-interval *seconds* / hello-interval *seconds* / retransmit-interval *seconds* / transmit-delay *seconds*]	andatory. By default, no virtual link is created.

Note

- A virtual link must be configured between two ABRs.
- Two ABRs on which the virtual link is configured must be in the same public area. This area is also called the transit area of the virtual link.
- The transit area of a virtual link must not be a Stub area or NSSA area.

6.8.2.3 Configure OSPFv3 Network Type

According to the link protocol types, OSPFv3 classifies networks into four types:

- Broadcast Network: When the link protocol of the network is Ethernet or Fiber Distributed Data Interface (FDDI), the default OSPFv3 network type is broadcast.
- Point To Point Network (P2P Network): When the link protocol is Point to Point Protocol (PPP), Link Access Procedure Balanced (LAPB), or High-level Data Link Control (HDLC), the default OSPFv3 network type is P2P.
- Non-Broadcast Multi-Access Network (NBMA Network): When the link protocol is ATM, frame relay, or X.25, the default OSPFv3 network type is NBMA.
- Point To Multi-Point Network (P2MP): No link protocol will be regarded by OSPFv3 as the P2MP network by default. Usually, the NBMA network that is not totally connected is configured as the OSPFv3 P2MP network.

You can modify the network type of an OSPFv3 interface according to the actual requirement. The network types of the interfaces through which OSPFv3 neighbors are set up must be the same; otherwise, normal learning of routes is affected.

Configuration Condition

Before configuring the OSPFv3 network type, ensure that:

- Enable the IPv6 forwarding function
- Enable the OSPFv3 protocol

Configure the Network Type of an OSPFv3 Interface to Broadcast

A broadcast network supports multiple devices (more than two devices). These devices can exchange information with all the devices in the network. OSPFv3 uses Hello packets to dynamically discover neighbors.

Table 621 Configure the network type of an OSPFv3 interface to broadcast

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the network type of an OSPFv3 interface to broadcast.	ipv6 ospf network broadcast	Mandatory. By default, the network type of an OSPFv3 interface is determined by the link layer protocol.

Configure the Network Type of an OSPFv3 Interface to P2P

A P2P network is a network that consists of two devices. Each device is located at one end of a P2P link. OSPFv3 uses Hello packets to dynamically discover neighbors.

Table 622 Configure the network type of an OSPFv3 interface to P2P

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the OSPFv3 network type to P2P.	ipv6 ospf network point-to-point	Mandatory. By default, the network type of an OSPFv3 interface is determined by the link layer protocol.

Configure the Network Type of an OSPFv3 Interface to NBMA

An NBMA network supports multiple devices (more than two devices), but the

devices does not have the broadcast capability, therefore, you must specify a neighbor manually.

Table 623 Configure the network type of an OSPFv3 interface to NBMA

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the network type of the OSPFv3 interface to NBMA.	ipv6 ospf network non-broadcast	Mandatory. By default, the network type of an OSPFv3 interface is determined by the link layer protocol.
Configure a neighbor for the NBMA network.	ipv6 ospf neighbor *neighbor-ipv6-address* [priority *priority-value* / poll-interval *interval-value* / cost *cost-value*] [instance-id *instance-id*]	Mandatory. In an NBMA network, a neighbor must be specified manually.

Configure the Network Type of an OSPFv3 Interface to P2MP

When an NBMA network is not fully connected, you can configure its network type to P2MP to save network overhead. If the network type is configured to P2MP unicast, you need to specify a neighbor manually.

Table 624 Configure the network type of an OSPFv3 interface to P2MP

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

Step	Command	Description
configuration mode.		
Configure the OSPFv3 network type to P2MP.	ipv6 ospf network point-to-multipoint [non-broadcast]	andatory. By default, the network type of an OSPFv3 interface is determined by the link layer protocol.
Configure a neighbor for the P2MP unicast network.	ipv6 ospf neighbor *neighbor-ipv6-address* [priority *priority-value* / poll-interval *interval-value* / cost *cost-value*] [instance-id *instance-id*]	If the interface network type is set to P2MP unicast, it is mandatory.

6.8.2.4 Configure OSPFv3 Network Authentication

To prevent information leakage or malicious attacks to OSPFv3 devices, all packet interaction between OSPFv3 neighbors has the authentication capability. The encrypted authentication types and algorithms include: NULL (no authentication), SHA1 authentication, and MD5 authentication, which is specified by the IPSec encrypted authentication policy.

After configuring authentication, IPSec security features encrypt and authenticate OSPFv3 protocol packets.The OSPFv3 protocol can receive packets only after decryption authentication. Therefore, the OSPFv3 interfaces which establish the adjacency relationship must have the same authentication method, Spi ID, and IPSec encryption authentication policy of authentication password configuration. The OSPFv3 authentication mode can be configured on the area and interface, and its priority is from low to high: area authentication, interface authentication. That is, first use the interface authentication mode, and then, use the area authentication mode.

Configuration Condition

Before configuring OSPFv3 network authentication, ensure that:

The IPv6 forwarding function is enabled.

The OSPFv3 protocol is enabled.

Configure OSPFv3 Area Authentication

Configuring the area authentication in the OSPFv3 process area can make all interfaces in the area use the area authenticaton mode, and effectively avoid configuring the same network authentication mode in the interface repeatedly.

Table 625 Configure OSPFv3 area authentication

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the area authentication mode.	area *area-id* ipsec-tunnel *tunnel-name*	Mandatory By default, OSPFv3 is not configured with the area authentication.

Configure OSPFv3 Interface Authentication

If an interface has multiple OSPFv3 instances, you can specify the authentication mode and password for one instance. If you do not specify the interface authentication instance in the interface, adopt the specified authentication mode in the area.

Table 626 Configure OSPFv3 interface authentication

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

Configure the interface authentication mode.	ipv6 ospf ipsec-tunnel tunnel-name{instance-id instance-id}	Mandatory By default, OSPFv3 is not configured with the interface authentication mode.

6.8.2.5 Configure OSPFv3 Route Generation

Configuration Condition

Before configuring OSPFv3 route generation, ensure that:

The IPv6 forwarding function is enabled.

- The OSPFv3 protocol is enabled.

Configure OSPFv3 Route Re-distribution

If multiple routing protocols run on one device, routes of other protocols can be introduced to OSPF through redistribution. By default, class-2 external routes of OSPFv3 are generated with the route metric 20. When you introduces external routes through redistribution, you can modify the external route type, metric, and tag field, and associate the specified routing policy to perform route control and management.

Table 627 Configure OSPFv3 route re-distribution

Step	Command	Description
Enter the 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-*	Mandatory By default, OSPFv3 is not configured with the route re-distribution.

Step	Command	Description
	type]	
Configure the metric of the OSPFv3 external route.	default-metric *metric-value*	Optional

Note

- If the metric value of external routes are configured by using both the redistribute protocol [protocol-id] metric command and the default-metric command, the value that is configured by using the former command has a higher priority.

Configure OSPFv3 Default Route

After an OSPFv3 Stub area or a totally NSSA areas is configured, a Type-3 default route is generated. For an NSSA area, no default route is automatically generated. You can use the **area** *area-id* **nssa default-information-originate** command to introduce a Type-7 default route to the NSSA area.

OSPFv3 cannot use the **redistribute** command to introduce a Type-5 default route. To do this, use the **default-information originate** [**always**] command.

Table 628 Configure the default OSPFv3 route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPFv3 to introduce a default route.	default-information originate [always / metric *metric-value* /	Mandatory. By default, no external default

Step	Command	Description
	metric-type *metric-type* / route-map *route-map-name*]	route is introduced to an OSPFv3 AS. The default metric of the introduced default route is 1, and the type is external type 2. The field always means to force the OSPFv3 AS to generate a default route; otherwise, the default route is generated only when there is a default route in the local routing table.

6.8.2.6 Configure OSPFv3 Route Control

Configuration Condition

Before configuring OSPFv3 route control, ensure that:

The IPv6 forwarding function is enabled.

- The OSPFv3 protocol is enabled.

Configure Route Summary between OSPFv3 Areas

When an ABR in OSPFv3 advertises inter-area routes to other areas, it advertises each route separately in the form of Type-3 LSA. You can use the inter-area route summary function to summarize some continuous network segments to form a summary route. Then the ABR advertises the summary route, reducing the size of OSPFv3 databases.

Table 629 Configure route summary between OSPFv3 areas

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the route summary between OSPFv3 areas	area *area-id* range ipv6-*prefix*/*prefix-length* [advertise | not-advertise]	Mandatory By default, ABR does not perform the route summary between the areas.

Note

- The route summary function between OSPFv3 areas is valid only for ABRs.
- By default, the minimum cost value among the cost values of the routes is used as the cost value of the route summary.

Configure OSPFv3 External Route Summary

When OSPF redistributes external routes, it advertises each route separately in the form of external LSA. You can use the external route summary function to summarize some continuous network segments to form a summary route. Then OSPF advertises the summary route, reducing the size of OSPF databases.

If you run the **summary-address** command on an ASBR, you can summarize all Type-5 LSAs and Type-7 LSAs within the address range.

Table 630 Configure OSPFv3 external route summary

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPFv3 to summarize external routes.	summary-prefix *ipv6-prefix/prefix-length* [not-advertise | tag *tag-value*]	Mandatory. By default, an ABR does not summarize external routes.

Note

- The OSPFv3 external route summary function is valid only for ASBRs.

Configure Route Filtering between OSPFv3 Areas

When an ABR receives inter-area routes, it performs filtration in the incoming direction based on an ACL or prefix list. When the ABR advertises inter-area routes, it performs filtration in the outgoing direction based on an ACL or prefix list.

Table 631 Configure route filteringbetween OSPFv3 areas

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the route filtering between OSPFv3 areas	area *area-id* filter-list { access { *access-list-name* | *access-list-number* } | prefix *prefix-list-name* } { in | out }	Mandatory By default, ABR does not perform the route filtering between areas.

Note

- The OSPFv3 inter-area route filtering function is valid only for ABRs.

Configure OSPFv3 External Route Filtration

Configuring OSPFv3 external route filtering is to apply an ACL or prefix list to allow or not allow external routes of an OSPFv3 AS to flood into the OSPF AS.

Table 632 Configure OSPFv3 external route filtration

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPFv3 external route filtering	distribute-list { access { *access-list-name* | *access-list-number* } | prefix *prefix-list-name* } out [*routing-protocol* [*process-id*]]	Mandatory By default, ASBR does not perform the external route filtering.

Note

- The OSPFv3 external route filtering function is valid only for ASBRs.

Configure OSPFv3 Route Installation Filtration

After OSPFv3 calculates routes through LSA, to prevent certain routes from being added into the routing table, OSPFv3 filters the calculated OSPFv3 route information.

Table 633 Configure OSPFv3 route installation filtration

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPFv3 route installation filtering	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*]	Mandatory By default, do not configure OSPFv3 route installation filtering.

Note

- Filtration based on prefix, gateway, and route-map is mutually exclusive with filtration based on ACL. For example, if you have configured filtration based on prefix, you cannot configure filtration based on ACL again.
- Filtration based on route-map and prefix is mutual exclusive with filtration based on gateway.
- Filtration based on prefix and filtration based on gateway overwrite each other.

Configure the Cost Value of an OSPFv3 Interface

By default, the cost of an OSPFv3 interface is calculated based on the following formula: Reference bandwidth/Interface bandwidth.

Table 634 Configure the cost value of an OSPFv3 interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the cost value of an OSPFv3 interface.	ipv6 ospf cost *cost* [instance-id *instance-id*]	Optional. By default, the cost value is calculated through the formula Reference bandwidth/Interface bandwidth.

Configure the OSPFv3 Reference Bandwidth

The reference bandwidth of an interface is used to calculate the cost value of the interface. The default value is 100Mbit/s. The formula for calculating the cost value of the OSPFv3 interface is: Reference bandwidth/Interface bandwidth. If the calculation result is larger than 1, use the integer part. If the calculation result is smaller than 1, use the value 1. Therefore, in a network whose bandwidth is larger than 100Mbit/s, the optimal route fails to be selected. In this case, you can use the **auto-cost reference-bandwidth** command to configure a proper reference bandwidth to solve the problem.

Table 635 Configure the OSPFv3 reference bandwidth

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configuring the OSPFv3 reference bandwidth.	auto-cost reference-bandwidth *reference-bandwidth*	Optional. By default, the reference

Step	Command	Description
		bandwidth is 100Mbit/s

Configure the OSPFv3 Administrative Distance

An administrative distance is used to indicate the reliability of the routing protocol. If the routes to the same destination network are learnt by different routing protocols, the route with the smallest administrative distance is selected first.

Table 636 Configure the OSPFv3 administrative distance

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPFv3 administrative distance.	distance [ospf { external *distance* / inter-area *distance* / intra-area *distance* } | *distance*]	Optional. By default, the administrative distance of intra-area and inter-area OSPFv3 routes is 110, and the administrative distance of external routes is 150

Configure the Maximum Number of OSPFv3 Load Balancing Routes

If multiple equivalent paths are available to reach the same destination, load balancing is achieved. This improves the utility rate of links and reduces the load of the links.

Table 637 Configure the maximum number of OSPFv3 load balancing routes

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

Step	Command	Description
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the maximum number of OSPFv3 load balancing routes.	maximum-paths *max-number*	Optional. By default, the maximum number of OSPFv3 load balancing routes is 4.

6.8.2.7 Configure OSPFv3 Network Optimization

Configuration Condition

Before configuring OSPFv3 network optimization, ensure that:

The IPv6 forwarding function is enabled.

- The OSPFv3 protocol is enabled.

Configure the Keep-alive Time of an OSPFv3 Neighbor

OSPFv3 Hello packets are used to set up neighbor relations and keep the relations alive. The default transmission interval of Hello packets is determined by the network type. For broadcast networks and P2P networks, the default transmission interval of Hello packets is 10s. For P2MP networks and NBMA networks, the default transmission interval of Hello packets is 30s.

Neighbor dead time is used to determine the validity of a neighbor. By default, the neighbor dead time is four times the Hello interval. If an OSPFv3 device fails to receive Hello packets from a neighbor after the neighbor dead time times out, the OSPFv3 device regards the neighbor as invalid, and then it deletes the neighbor in an active manner.

Table 638 Configure the keep-alive time of an OSPFv3 neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface interface-name	-
Configure an OSPFv3 Hello interval.	ipv6 ospf hello-interval interval-value [instance-id instance-id]	Optional. The default value is determined by the network type. For broadcast networks and P2P networks, the default value is 10s. For P2MP networks and NBMA networks, the default value is 30s.
Configure the OSPFv3 neighbor dead time.	ipv6 ospf dead-interval interval-value [instance-id instance-id]	Optional. By default, the dead time is four times of the Hello interval.

Note

- The Hello interval and neighbor dead time of OSPFv3 neighbors must be the same; otherwise, they cannot set up neighbor relations.
- When you modify the Hello interval, if the current neighbor dead time is four times of the Hello interval, the neighbor dead time is automatically modified to be still four times of the new Hello interval. If the current neighbor dead time is not four times of the Hello interval, the neighbor dead time keeps unchanged.
- If you modify the neighbor dead time, the Hello interval is not affected.

Configure an OSPFv3 Passive Interface

The dynamic routing protocol adopts a passive interface to effectively decrease the network bandwidth consumed by the routing protocol. After an OSPFv3 passive interface is configured, you can use the **enable** command of the interface to advertise the routes of the directly connected network segment in which the interface is located, but the receiving and transmitting of OSPFv3 packets are damped on the interface.

Table 639 Configure an OSPFv3 passive interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure an OSPFv3 passive interface.	passive-interface {*interface-name*|default}	Mandatory. By default, no OSPFv3 passive interface is configured.

Configure an OSPFv3 Demand Circuit

On P2P and P2MP links, to decrease the line cost, you can configure an OSPFv3 demand circuit to suppress periodical transmitting of Hello packets and periodical update of LSA packets. This function is mainly applied on charged links such as ISDN, SVC, and X.25.

Table 640 Configure an OSPFv3 demand circuit

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

Step	Command	Description
Configure an OSPFv3 demand circuit.	ipv6 ospf demand-circuit [instance-id *instance-id*]	Mandatory. By default, no OSPFv3 demand circuit is enabled.

Configure the Priority of an OSPFv3 Interface

Interface priorities are mainly used in election of Designated Router (DR), and Backup Designated Router (BDR) in broadcast networks and NBMA networks. The value range is 0-255. The larger the value is, the higher the priority is. The default value is 1.

The DR and BDR are selected from all devices in a network segment based on interface priorities and Router IDs through Hello packets. The rules are as follows:

- First, the device whose interface has the highest priority is elected as the DR, and the device whose interface has the second highest priority is elected as the BDR. The device whose interface has the priority 0 does not participate in the election.
- If the interface priorities of two devices are the same, the device with the largest Router ID is elected as the DR, and the device with the second largest Router ID is elected as the BDR.
- If the DR fails, the BDR becomes the DR immediately, and a new BDR is elected.

Table 641 Configure the priority of an OSPFv3 interface

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

Step	Command	Description
Enter the interface configuration mode.	interface *interface-name*	-
Configure the priority of an OSPFv3 interface.	ipv6 ospf priority *priority-value* [instance-id *instance-id*]	Optional. By default, the OSPFv3 interface priority is 1.

Note

- Interface priorities affect only an election process. If the DR and BDR have already been elected, modification of interface priorities does not affect the election result; instead, it affects the next election of DR or BDR. Therefore, the DR may not have the interface with the highest priority, and the BDR may not have the interface with the second highest priority.

Configure the OSPFv3 Interface to Ignore MTU

When adjacent OSPF devices exchange DD packets, MTUs are checked by default. If the MTUs are different, the devices cannot form a neighbor relation. If you have configured OSPFv3 to ignore interface MTU check, even if MTUs are different, they can set up a neighbor relation.

Table 642 Configure an OSPFv3 interface to ignore MTU

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the OSPFv3	ipv6 ospf mtu-ignore [instance-	Mandatory

Step	Command	Description
interface to ignore MTU.	id *instance-id*]	By default, the OSPFv3 interface performs the MTU consistency check.

Configure the LSA Transmit Delay of an OSPFv3 Interface

LSA transmit delay refers to the time it takes for an LSA to flood to other devices. The device that sends the LSA adds the interface transmit delay to the LSA aging time. By default, once the flooding LSA passes a device, the aging time is increased by 1. You can configure the LSA transmit delay according to the network conditions. The value range is 1-840. LSA transmit delay is usually configured on low-speed links.

Table 643 Configure the LSA transmit delay of an OSPFv3 interface

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the LSA transmit delay of an OSPFv3 interface.	ipv6 ospf transmit-delay *delay-value* instance-id [*instance-id*]	Optional. By default, the LSA transmit delay is 1s.

Configure OSPFv3 LSA Retransmission

To ensure the reliability of data exchange, OSPFv3 adopts the acknowledgement mechanism. If an LSA floods on a device interface, the LSA is added into the retransmission list of the neighbor. If no acknowledgement message is received from the neighbor after the retransmission time times out, the LSA is retransmitted until an acknowledgement message is received.

Table 644 Configure OSPFv3 LSA retransmission

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the interval of OSPFv3 LSA retransmission.	ipv6 ospf retransmit-interval *interval-value* [instance-id *instance-id*]	Optional. By default, the retransmission interval is 5s.

Configure OSPFv3 SPF Calculation Time

If the OSPFv3 network topology changes, routes need to be re-calculated. When the network continues to change, frequent route calculation occupies a lot of system resources. You can adjust the SPF calculation time parameters to prevent frequent network changes from consuming too many system resources.

Table 645 Configure OSPFv3 SPF calculation time

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPFv3 SPF calculation 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* indicates the initial calculation delay, *hold-time* indicates the suppression time, and *max-time* indicates the maximum waiting time between two SPF calculations. If network changes are not frequent, you can shorten the continuous route calculation interval to *delay-time*. If network changes are frequent, you can adjust the parameters, increase the suppression time to *hold-time*×2^{n-2} (n is the number of route calculation trigger times), extend the waiting time based on the configured *hold-time* increment and the maximum value must not exceed *max-time*.

6.8.2.8 Configure OSPFv3 Fast Re-Routing

Configuration Conditions

Before configuring the OSPFv3 fast re-routing, first complete the following task:

- Enable the IPv6 forwarding function
- Enable the OSPFv3 protocol

Configure OSPFv3 Fast Re-routing

In OSPFv3 network, due to link or device failure, the packets passing through the failure point will be discarded or a loop will be generated. The traffic interruption caused by this will continue until the protocol re-converges, which often lasts for several seconds. In order to reduce the traffic interruption time, OSPFv3 fast rerouting can be configured. By applying the route map, the backup next hop can be set for the successfully matched route. Once the main link fails, the traffic passing through the failed link will be immediately switched to the backup link, so as to realize fast switching.

Table-646 Configure OSPFv3 fast re-routing

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure the OSPFv3 process to enable the static fast re-routing function	fast-reroute route-map *route-map-name*	Mandatory By default, do not enable the OSPFv3 static fast re-routing function.
Configure the OSPFv3 process to enable the dynamic fast re-routing function	fast-reroute loop-free-alternate [route-map *route-map-name*]	Mandatory By default, do not enable the OSPFv3 dynamic fast re-routing function.
Configure the OSPFv3 process to enable the pic function	pic	Mandatory After enabling the pic function, enable the auto fast re-routing function. By default, do not enable the OSPFv3 pic function.

Note

- OSPFv3 fast re-routing function can be divided into static fast rerouting and dynamic fast rerouting.
- The static fast rerouting function needs to associate the route map, and set the next hop interface and address of the backup route in the route-map.
- At present, dynamic fast rerouting only supports point-to-point network, that is, the network type of all outgoing interfaces of the device needs to be point-

to-point. After configuring dynamic fast rerouting, the device automatically calculates and sets the backup next hop interface and address. Dynamic fast rerouting can also be associated with route-map. Only the routes matching route map are set to back up the next hop interface and address.

- The various modes of enabling rerouting are mutually exclusive.

6.8.2.9 Configure OSPFv3 GR

GR (Graceful Restart) is used to keep the route information of the forwarding layer between the local device and the neighbor device unchanged during the active/standby switchover of the devices and the forwarding is not affected. After switching the device and running again, the protocol layer of the two devices synchronizes the route information and updates the forwarding layer so that the data forwarding is not interrupted during the device switchover.

There are two roles during GR:

- GR Restarter: The device performing the protocol graceful restarting
- GR Helper: The device assisting the protocol graceful restarting

The distributed device can serve as GR Restarter and GR Helper, while the centralized device can only serve as GR Helper, assisting Restarter to complete GR.

Configuration Condition

Before configuring OSPFv3 GR, first complete the following task:

- The IPv6 forwarding function is enabled.
- The OSPFv3 protocol is enabled.

Configure OSPFv3 GR Restarter

Table -647 Configure OSPFv3 GR Restarter

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Configure OSPFv3 GR	nsf ietf	Mandatory By default, do not enable GR function. The function takes effect and the protocol needs to support the Opaque-LSA function. By default, support the Opaque-LSA function.
Configure OSPFv3 GR period	nsf interval *grace-period*	Optional By default, the GR period is 120s.

Note

- The OSPFv3 GR function can be used only in the stacking environment or dual-control environment.

Configure OSPFv3 GR Helper

GR Helper helps Restarter to complete GR. By default, the device enables the function. The **nsf ietf helper disable** command is used to disable the GR Helper function. The **nsf ietf helper strict-lsa-checking** command is used to configure Helper to perform the strict check for LSA during GR. If finding that the LSA does not change, exit the GR Helper mode.

Table 648 Configure OSPFv3 GR Helper

Step	Command	Description
Enter the 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, enable the Helper function and do not perform the strict check for LSA

6.8.2.10 Configure OSPFv3 to Coordinate with BFD

Configuration Condition

Before configuring OSPFv3 to coordinate with BFD, ensure that:

The IPv6 forwarding function is enabled.

- The OSPFv3 protocol is enabled.

Configure OSPFv3 to Coordinate with BFD

Bidirectional Forwarding Detection (BFD) provides a method for quickly detecting the status of a line between two devices. If BFD is started between two adjacent OSPFv3 devices, if the line between two devices becomes faulty, BFD quickly detects the fault and informs OSPFv3 of the fault. Then, it triggers OSPFv3 to start route calculation and switch over to the backup line, achieving fast switchover of routes.

Table 649 Configure OSPFv3 to coordinate with BFD

Step	Command	Description

Enter the global configuration mode.	configure terminal	-
Enter the interface configuration mode.	interface *interface-name*	-
Enable or disable BFD on the specified OSPFv3 interface.	ipv6 ospf bfd [disable] [instance-id *instance-id*]	Mandatory. By default, the BFD function is disabled.
Enter the global configuration mode.	exit	-
Enter the OSPFv3 configuration mode.	ipv6 router ospf *process-id* [vrf *vrf-name*]	-
Enable BFD on all interfaces of the OSPFv3 process.	bfd all-interfaces	Optional

Note

- If BFD is configured both in OSPFv3 configuration mode and interface configuration mode, the BFD configuration in the interface has the higher priority.

6.8.2.11 OSPFv3 Monitoring and Maintaining

Table 650 OSPFv3 monitoring and maintaining

Command	Description
clear ipv6 ospf err-statistic	Clear the OSPFv3 error statistics information.
clear ipv6 ospf [*process-id*] process	Reset an OSPFv3 process.

Command	Description
clear ipv6 ospf [*process-id*] redistribution	Re-advertise external routes.
clear ipv6 ospf [*process-id*] route	Re-calculate OSPFv3 routes.
clear ipv6 ospf statistics [*interface-name*]	Clear the OSPFv3 interface statistics information
show ipv6 ospf [*process-id*]	Display the OSPFv3 basic information.
show ipv6 ospf [*process-id*] border-routers	Display the information about the routes to the boundary devices in OSPFv3.
show ipv6 ospf core-info	Display the core information of the 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]	Display the information about an OSPFv3 database.
show ipv6 ospf error-statistic	Display the OSPFv3 error statistics information
show ipv6 ospf event-list	Display the receiving queue information of the OSPFv3 packet
show ipv6 ospf interface [*interface-name* [detail]]	Display the information about an OSPFv3 interface.
show ipv6 ospf [*process-id*] neighbor [*neighbor-id* | all | detail [all] | interface *interface-name* [detail] | statistics]	Display the information about OSPFv3 neighbors.
show ipv6 ospf [*process-id*] route [*ipv6-prefix/prefix-length* | connected | external | inter-area | intra-area | statistic]	Display the information about OSPFv3 routes.

Command	Description
show ipv6 ospf [*process-id*] sham-link	Display the configured OSPFv3 sham link information about, including interface status, cost value, and neighbor status.
show ipv6 ospf [*process-id*] topology area [*area-id*]	Display the OSPFv3 topology information
show ipv6 ospf [*process- id*] virtual-links	Display the OSPFv3 virtual link information
show ipv6 ospf [vrf *vrf-name*]	Display the all OSPFv3 process information and parameters in the specified vrf
show running-config ipv6 router ospf	Display the OSPFv3 running configuration

6.8.3 OSPFv3 Typical Configuration Example

6.8.3.1 Configure OSPFv3 Basic Functions

Network Requirements

- Configure the OSPFv3 protocol for all devices, and divide the devices into three areas: Area 0, Area 1, and Area 2. After configuration, all devices should be able to learn routes from each other.
- On a back-to-back Ethernet interface, to speed up set of OSPFv3 neighbors, you can change the network type of the OSPFv3 interface to P2P. Modify the network type of the interfaces in Area 2 to P2P. After the configuration, all devices can learn routes from each other.

Network Topology

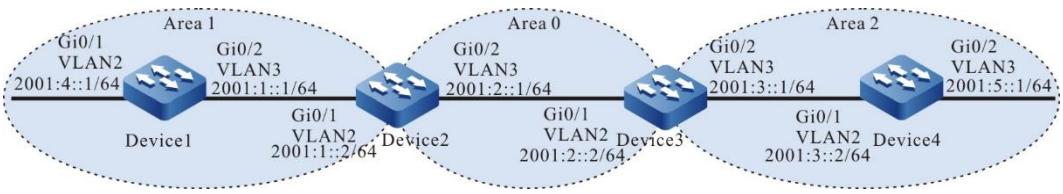


Figure 131 Networking for configuring basic OSPFv3 functions

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IPv6 addresses of the interfaces. (Omitted)

Step 3: Configure an OSPFv3 process and let the interface cover different areas.

#On Device1, configure an OSPFv3 process and configure the interfaces to cover 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
```

#On Device2, configure an OSPFv3 process and configure the interfaces to cover Area 0 and Area 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
```

#On Device3, configure an OSPFv3 process and configure the interfaces to cover Area 0 and Area 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
```

#On Device4, configure an OSPFv3 process and configure the interfaces to cover 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

- The Router ID in OSFPv3 must be configured manually, and the Router IDs of any two routers in the AS cannot be the same.
- When an interface is enabled to OSPFv3, it is necessary to specify which interface instance is enabled to the OSPFv3 process, and the two instance numbers should be consistent. By default, it is 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 ::, 00:41:07, lo0
C   2001:1::/64 [0/0]
     via ::, 00:32:19, vlan3
L   2001:1::1/128 [0/0]
     via ::, 00:32:18, lo0
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fe5e:6d45, 00:23:06, vlan3
O   2001:3::/64 [110/3]
     via fe80::201:7aff:fe5e:6d45, 00:23:00, vlan3
C   2001:4::/64 [0/0]
     via ::, 00:16:46, vlan2
L   2001:4::1/128 [0/0]
     via ::, 00:16:45, lo0
O   2001:5::/64 [110/4]
     via fe80::201:7aff:fe5e:6d45, 00:01:42, vlan3
```

#Query the OSPFv3 neighbors 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         00:00:33    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 ::, 00:50:36, lo0
C   2001:1::/64 [0/0]
     via ::, 00:43:05, vlan2
L   2001:1::2/128 [0/0]
     via ::, 00:43:04, lo0
C   2001:2::/64 [0/0]
     via ::, 00:40:01, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:39:57, lo0
O   2001:3::/64 [110/2]
     via fe80::2212:1ff:fe01:101, 00:34:00, vlan3
O   2001:4::/64 [110/2]
```

```
    via fe80::201:7aff:fe61:7a24, 00:27:28, vlan2
O   2001:5::/64 [110/3]
    via fe80::2212:1ff:fe01:101, 00:12:41, vlan3
```

#Query OSPFv3 Link Status Database (LSDB) 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, routes 2001:3::/642 and 2001:5::/64 are inter-area routes. You can query the LSA information of the related routes in Inter-Area-Prefix-LSA (Area 0.0.0.0). In the case of intra-area routes, run the **show ipv6 ospf database intra-prefix** command to query the LSA information of the related routes.

Step 4: Configure the network type of OSPFv3 interfaces to P2P.

#On Device3, configure the OSPFv3 network type of interface vlan3 to P2P.

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#On Device4, configure the OSPFv3 network type of 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 neighbors 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:09:10:10, lo0
O   2001:1::/64 [110/2]
     via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
C   2001:2::/64 [0/0]
     via ::, 03:07:51, vlan2
L   2001:2::2/128 [0/0]
     via ::, 03:07:48, lo0
C   2001:3::/64 [0/0]
     via ::, 03:07:41, vlan3
L   2001:3::1/128 [0/0]
     via ::, 03:07:39, lo0
O   2001:4::/64 [110/3]
     via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
O   2001:5::/64 [110/2]
     via fe80::201:2ff:fe03:405, 00:00:22, vlan3
```

Note

- If OSPFv3 neighbor relations are set up in a P2P network, no DR or BDR election will be performed.

#Query the OSPFv3 neighbors 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 ::, 00:05:34, lo0
O   2001:1::/64 [110/3]
     via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
O   2001:2::/64 [110/2]
     via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C   2001:3::/64 [0/0]
     via ::, 00:04:34, vlan2
L   2001:3::2/128 [0/0]
     via ::, 00:04:31, lo0
O   2001:4::/64 [110/4]
     via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C   2001:5::/64 [0/0]
     via ::, 00:03:14, vlan3
L   2001:5::1/128 [0/0]
     via ::, 00:03:13, lo0
```

After the network type of OSPFv3 interfaces are modified to P2P, neighbors can be set up normally, and routes can be learned normally.

6.8.3.2 Configure OSPFv3 to Use IPSec Encryption Authentication

Network Requirements

- All routers run OSPFv3, and the whole AS is divided to two areas.
- Device1, Device2, and Device3 use the IPsec tunnel to perform the encryption authentication for the OSPFv3 protocol packets; Device1 and Device2 adopt the ESP transmission encapsulation mode, the encryption algorithm is 3des, and the authentication algorithm is sha1; Device2 and Device3 adopt the ESP transmission encapsulation mode, the encryption algorithm is aes128, and the ESP authentication algorithm is sm3.
- After configuration, the device can normally set up the neighbor and lear

the routes from each other.

Network Topology

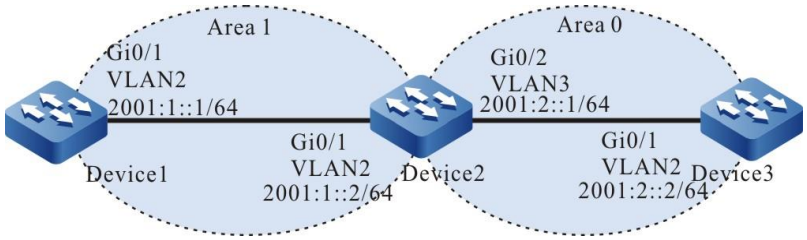


Figure 132 Networking for configuring OSPFv3 to use the IPSec encryption authentication

Configuration Steps

Step 1: Configure the IPv6 addresses of the interfaces. (Omitted)

Step 2: Configure an OSPFv3 process, and enable the OSPFv3 function on the corresponding interface.

#Configure the OSPFv3 process of Device1, Device2, and Device3, and enable OSPFv3 on 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 the IPSec proposal and manual tunnel.

#Configure Device1, create the IPSec proposal a, adopt the ESP transmission encapsulation mode, encryption algorithm 3des, and authentication algorithm sha1, create 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 ipv6-tunnel a manual
Device1(config-manual-tunnel-ipv6)#set ipsec proposal a
Device1(config-manual-tunnel-ipv6)#set inbound esp 1000 encryption 0 11111111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaa
Device1(config-manual-tunnel-ipv6)#set outbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaa authentication 0 1111111111111111
Device1(config-manual-tunnel-ipv6)#exit
```

#Configure Device2, create the IPSec proposal a, adopt the ESP transmission encapsulation mode, encryption algorithm 3des, and authentication algorithm sha1, create IPSec manual tunnel a, and configure the SPI and key ; create IPSec proposal b, adopt the ESP transmission encapsulation mode, encryption algorithm aes128, and authentication algorithm sm3, create 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 ipv6-tunnel a manual
Device2(config-manual-tunnel-ipv6)#set ipsec proposal a
Device2(config-manual-tunnel-ipv6)#set inbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaa authentication 0 1111111111111111
Device2(config-manual-tunnel-ipv6)#set outbound esp 1000 encryption 0 11111111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaa
```

```
Device2(config-manual-tunnel-ipv6)#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 ipv6-tunnel b manual
Device2(config-manual-tunnel-ipv6)#set ipsec proposal b
Device2(config-manual-tunnel-ipv6)#set inbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Device2(config-manual-tunnel-ipv6)#set outbound esp 2000 encryption 0 1111111111111111 authentication 0 11111111111111111111111111111111
Device2(config-manual-tunnel-ipv6)#exit
```

#Configure Device3, create the IPSec proposal b, adopt the ESP transmission encapsulation mode, encryption algorithm aes128, and authentication algorithm sm3, create 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 ipv6-tunnel b manual
Device3(config-manual-tunnel-ipv6)#set ipsec proposal b
Device3(config-manual-tunnel-ipv6)#set inbound esp 2000 encryption 0 1111111111111111 authentication 0 11111111111111111111111111111111
Device3(config-manual-tunnel-ipv6)#set outbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Device3(config-manual-tunnel-ipv6)#exit
```

Step 4: In the OSPFv3 process, the areas are bound to the corresponding IPSec tunnel.

#In the OSPFv3 process of Device1, area 1 is bound to IPSec tunnel a.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#area 1 ipsec-tunnel a
Device1(config-ospf6)#exit
```

#In the OSPFv3 process of Device2, area 1 is bound to IPSec tunnel a, and area 0 is bound 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
Device2(config-ospf6)#exit
```

#In the OSPFv3 process of Device3, area 0 is bound 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.

#View 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
```

You can see that the area is bound to IPSec tunnel a, and the ID is a random value of 0-1023.

#View the IPSec tunnel information of Device1.

```
Device1# show crypto ipv6-tunnel a
get the manual ipv6 tunnel
Crypto tunnelv6 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
```

You can see that route rt_id is equal to the ID in show ipv6 ospf 100.

#View the IPSec tunnel encryption type information of Device1.

```
Device1#show crypto ipsec sa ipv6-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
```

You can see that IPSec tunnel a adopts the ESP transmission encapsulation mode, encryption algorithm 3des, and authentication algorithm sha1.

#View 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 00:00:06
  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
```

You can see that the interface is bound to IPSec tunnel a, and the ID is a random value of 0-1023.

#View the OSPFv3 neighbor information and core route 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:04:06:36, lo0
C   2001:1::/64 [0/0]
     via ::, 03:00:53, vlan2
L   2001:1::1/128 [0/0]
     via ::, 03:00:49, lo0
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec9:1cdd, 2d:00:03:49, vlan2
```

On Device1, the neighbor is normally set up, and the route is learnt normally.

#View the OSPFv3 process 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
```

You can see that the area is bound to IPSec tunnel b, and the ID is a random value of 0-1023.

#View the IPSec tunnel information of Device3.

```
Device3# show crypto ipv6-tunnel b
get the manual ipv6 tunnel
Crypto tunnelv6 a : 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
```

You can see that route rt_id is equal to the ID in show ipv6 ospf 100.

#View the IPSec tunnel encryption type information of Device3.

```
Device3#show crypto ipsec sa ipv6-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
```

You can see that the IPSec tunnel adopts the ESP transmission encapsulation mode, encryption algorithm aes128, and authentication algorithm sm3.

#View 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 00:50:39, 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 00:00:02
 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
```

You can see that the interface is bound with the IPsec tunnel b, and the ID is a random value of 0-1023.

#View the OSPFv3 neighbor information and the core route 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  00:00:35       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 ::, 09:53:53, lo0
O   2001:1::/64 [110/2]
    via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C   2001:2::/64 [0/0]
    via ::, 03:05:16, vlan2
L   2001:2::2/128 [0/0]
    via ::, 03:05:13, lo0
```

On Device3, the neighbor is set up normally, and the route is learnt normally.

Step 6: Bind the OSPFv3 interface with the corresponding IPSec tunnel.

#Configure Device1, and bind the interface vlan2 with 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 with IPSec tunnel a; bind the interface vlan3 with 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 with 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.

#View 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 00:00:06
    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
```

You can see that the interface is bound with the IPsec tunnel a, and the ID is a random value of 0-1023.

#View the OSPFv3 core route 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:04:06:36, lo0
C   2001:1::/64 [0/0]
      via ::, 03:00:53, vlan2
L   2001:1::1/128 [0/0]
      via ::, 03:00:49, 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.

#View 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 00:50:39, 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 00:00:02
    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
```

You can see that the interface is bound with the IPsec tunnel b, and the ID is a random value of 0-1023.

#View the OSPFv3 core route 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 ::, 09:53:53, lo0
O   2001:1::/64 [110/2]
    via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C   2001:2::/64 [0/0]
    via ::, 03:05:16, vlan2
L   2001:2::2/128 [0/0]
    via ::, 03:05:13, lo0
```

On Device3, the route is learnt normally.

Note

- When configuring OSPFv3 to bind the IPSec tunnel, you can only configure the area binding or interface binding, and also can configure the area and interface binding at the same time.
- When the area binding and interface binding configure the IPSec tunnel at the same time, the interface binding takes effect first.

6.8.3.3 Configure OSPFv3 to Coordinate with BFD

Network Requirements

- Configure OSPFv3 for all devices.
- Enable the BFD detection function on the line between Device1 and Device3. If the line becomes faulty, BFD quickly detects the fault and notify OSPFv3 of the fault. Then, OSPFv3 switches the route to Device2 for communication.

Network Topology

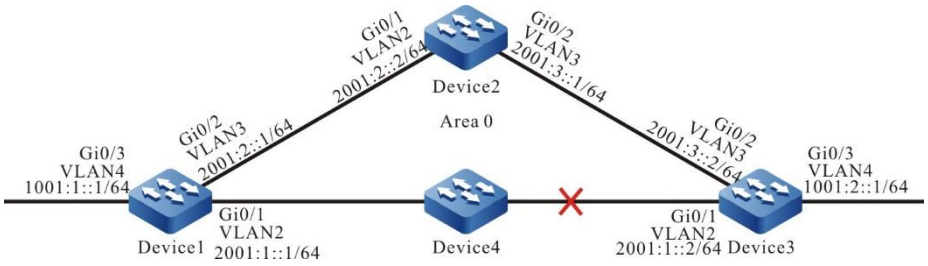


Figure 133 Networking for configuring OSPFv3 to coordinate with BFD

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN (omitted).

Step 2: Configure the IPv6 addresses of the interfaces. (Omitted)

Step 3: Configure an 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 coordinate 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.

#View the OSPFv3 neighbor information and route 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 00:00:37
   Neighbor is up for 00:01:31
   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 ::, 01:15:27, lo0
C   1001:1::/64 [0/0]
     via ::, 01:15:27, vlan4
L   1001:1::1/128 [0/0]
     via ::, 01:15:27, lo0
O   1001:2::/64 [110/2]
     via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
C   2001:1::/64 [0/0]
     via ::, 01:15:27, vlan2
L   2001:1::1/128 [0/0]
     via ::, 01:15:27, lo0
C   2001:2::/64 [0/0]
     via ::, 01:15:27, vlan3
L   2001:2::1/128 [0/0]
     via ::, 01:15:27, lo0
O   2001:3::/64 [110/2]
     via fe80::201:7aff:fe5e:6d45, 00:02:40, vlan3
           [110/2]
     via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
```

According to the OSPFv3 neighbor information, BFD has been enabled, and route 201.0.0.0/24 first selects the line between Device1 and Device3 for communication.

#View 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
```

OSPFv3 has successfully coordinated with BFD, and the session has been normally set up.

#If the line between Device1 and Device3 becomes faulty, BFD quickly detects the fault and informs OSPFv3 of the fault, and then, OSPFv3 switches the route to Device2 for communication. View the route 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 ::, 01:16:10, lo0
C   1001:1::/64 [0/0]
     via ::, 01:16:10, vlan4
L   1001:1::1/128 [0/0]
     via ::, 01:16:10, lo0
O   1001:2::/64 [110/3]
     via fe80::201:7aff:fe5e:6d45, 00:00:07, vlan3
C   2001:1::/64 [0/0]
     via ::, 01:16:10, vlan2
L   2001:1::1/128 [0/0]
     via ::, 01:16:10, lo0
C   2001:2::/64 [0/0]
     via ::, 01:16:10, vlan3
L   2001:2::1/128 [0/0]
     via ::, 01:16:10, lo0
O   2001:3::/64 [110/2]
     via fe80::201:7aff:fe5e:6d45, 00:03:22, vlan3
```

The action of Device3 is similar to that of Device1.

6.8.3.4 Configure OSPFv3 Static Fast Re-routing

Network Requirements

- All devices are configured with the OSPFv3 protocol.
- Enable static fast rerouting between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

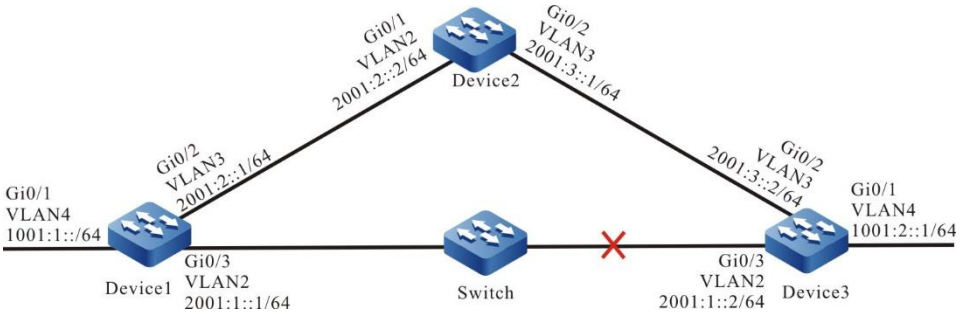


Figure 134 Networking of configuring OSPFv3 static fast re-routing

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN; configure the IPv6 address of the interface (omitted).

Step 2: 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
```

#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 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next hop interface vlan3, and the next hop address 2001:2:: 2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_ospf
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-nexthop 2001:2::2
Device1(config-route-map)#exit
```

Step 4: Configure the static fast re-routing.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#fast-reroute route-map ipv6frr_ospf
Device1(config-ospf6)#exit
```

Step 5: Check the result.

#View the OSPFv3 route 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 ::, 00:31:05, lo0
C   1001:1::/64 [0/0]
     via ::, 00:26:12, vlan4
L   1001:1::1/128 [0/0]
     via ::, 00:26:12, vlan4
O   1001:2::/64 [110/2]
     via fe80::201:7aff:fe92:e6b6, 00:22:11, vlan2
C   2001:1::/64 [0/0]
     via ::, 00:26:51, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:26:51, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:25:30, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:25:30, vlan3
O   2001:3::/64 [110/2]
     via fe80::201:7aff:fe92:e6b6, 00:20:53, vlan2
     via fe80::ced8:1fff:fe10:7aae, 00:21:06, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 FRR route table of Device1.

```
Device1#show ipv6 frr 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
O   1001:2::/64 [110/4294967295]
     via 2001:2::2, 00:03:16, vlan3
```

You can see that the next hop of the frr route 1001:2::/64 is 2001:2::2, and the outgoing interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr                 NeighAddr      LD/RD        State      Holddown    Interface
2001:1::1               2001:1::1      1017/1017    UP         500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:65  Remote Discriminator:65
Local State:UP  Remote State:UP  Up for: 0h:9m:11s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is associated with BFD successfully, the session is established normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 03:03:45, lo0
C   1001:1::/64 [0/0]
    via ::, 02:58:52, vlan4
L   1001:1::1/128 [0/0]
    via ::, 02:58:52, vlan4
O   1001:2::/64 [110/3]
    via fe80::ced8:1fff:fe10:7aae, 00:00:11, vlan3
C   2001:1::/64 [0/0]
    via ::, 02:59:31, vlan2
L   2001:1::1/128 [0/0]
    via ::, 02:59:31, vlan2
C   2001:2::/64 [0/0]
    via ::, 02:58:10, vlan3
L   2001:2::1/128 [0/0]
    via ::, 02:58:10, vlan3
O   2001:3::/64 [110/2]
    via fe80::ced8:1fff:fe10:7aae, 02:53:45, vlan3
```

6.8.3.5 Configure OSPFv3 Dynamic Fast Re-routing

Network Requirements

- All devices are configured with the OSPFv3 protocol.
- Enable dynamic fast rerouting between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

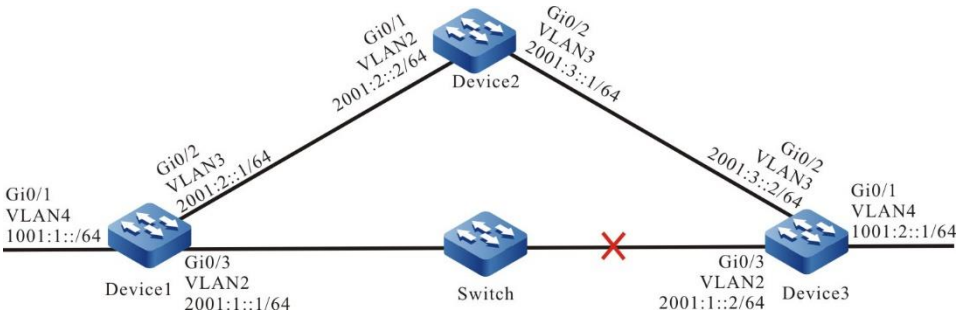


Figure 135 Networking of configuring OSPFv3 dynamic fast re-routing

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN; configure the IPv6 address of the interface (omitted).

Step 2: Configure the OSPFv3 process and configure the interface network type as point-to-point.

#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)# ipv6 ospf network point-to-point
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
```

```
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)# ipv6 ospf network point-to-point
Device1(config-if-vlan3)#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)# ipv6 ospf network point-to-point
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)# ipv6 ospf network point-to-point
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)# ipv6 ospf network point-to-point
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)# ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)# ipv6 ospf network point-to-point
Device3(config-if-vlan4)#exit
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to only match 1001:2::1/64, while the other segments are filtered.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
```

```
Device1(config)#route-map ipv6frr_ospf
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#exit
```

Step 4: Configure the dynamic fast re-routing.

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)# fast-reroute loop-free-alternate route-map ipv6frr_ospf
Device1(config-ospf6)#exit
```

Step 5: Check the result.

#View the OSPFv3 route 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 ::, 03:21:35, lo0
C   1001:1::/64 [0/0]
    via ::, 03:16:42, vlan4
L   1001:1::1/128 [0/0]
    via ::, 03:16:42, vlan4
O   1001:2::/64 [110/2]
    via fe80::201:7aff:fe92:e6b6, 00:01:35, vlan2
C   2001:1::/64 [0/0]
    via ::, 03:17:21, vlan2
L   2001:1::1/128 [0/0]
    via ::, 03:17:21, vlan2
C   2001:2::/64 [0/0]
    via ::, 03:16:00, vlan3
L   2001:2::1/128 [0/0]
    via ::, 03:16:00, vlan3
O   2001:3::/64 [110/2]
    via fe80::ced8:1fff:fe10:7aae, 00:07:50, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPV6 FRR route table of Device1.

```
Device1#show ipv6 frr 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
O   1001:2::/64 [110/4294967295]
      via fe80::ced8:1fff:fe10:7aae, 00:01:58, vlan3
```

You can see that the next hop of the frr route 1001:2::/64 is the linklocal address fe80:: ced8:1fff: fe10:7aae, and the outgoing interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1  detail
Total ipv6 session number: 1
OurAddr          NeighAddr      LD/RD        State      Holddown    Interface
2001:1::1        2001:1::1      1024/1024    UP         500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:66  Remote Discriminator:66
Local State:UP  Remote State:UP  Up for: 0h:4m:15s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is associated with BFD successfully, the session is established normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 03:03:45, lo0
C   1001:1::/64 [0/0]
      via ::, 02:58:52, vlan4
L   1001:1::1/128 [0/0]
      via ::, 02:58:52, vlan4
O   1001:2::/64 [110/3]
      via fe80::ced8:1fff:fe10:7aae, 00:00:11, vlan3
C   2001:1::/64 [0/0]
      via ::, 02:59:31, vlan2
L   2001:1::1/128 [0/0]
      via ::, 02:59:31, vlan2
C   2001:2::/64 [0/0]
```

```
    via ::, 02:58:10, vlan3
L   2001:2::1/128 [0/0]
    via ::, 02:58:10, vlan3
O   2001:3::/64 [110/2]
    via fe80::ced8:1fff:fe10:7aae, 02:53:45, vlan3
```

6.9 IS-IS

6.9.1 Overview

The IS-IS (Intermediate System to Intermediate System) is the IGP (Interior Gateway Protocol) based on the SPF algorithm . The basic design theory and algorithm for the IS-IS protocol are consistent with the OSPF. The IS-IS protocol is the routing protocol based on the link layer, which is irrelevant to the network layer (IPv4, IPv6, and OSI). It is not restricted by the network layer, and therefore it has good extensibility.

The IS-IS protocol can support the routing of multi-protocol stacks, including IPv4, IPv6, and OSI. The IS-IS protocol is initially applied to the OSI protocol stack (ISO10589) and then extended to the routing of IPv4 protocol stack (RFC1195) and IPv6 protocol stack (RFC5308).and, it can be further extended to support the CSPF calculation of the MPLS-TE (RFC3784).

The IS-IS protocol is characterized with good capability (inconsistent extended functions between devices can be compatible perfectly), large network capacity, able to support multi-protocol stacks, able to upgrade smoothly, unlikely to be faulty compared with the OSPF. Therefore, the IS-IS protocol applies to the large-size core backbone network. This section describes how to configure the IS-IS dynamic routing protocol on the device for network interconnection.

6.9.2 IS-IS Function Configuration

Table 651 IS-IS function list

Configuration Task	
Configure the IS-IS basic function	Enable the IS-IS protocol
	Configure the IS-IS VRF attribute
Configure the IS-IS layer attribute	Configure the IS-IS layer attribute
Configure the IS-IS route generation	Configure the IS-IS default route
	Configure the IS-IS routing redistribution
Configure the IS-IS routing control	Configure the IS-IS metric style
	Configure the IS-IS interface metric value
	Configure the IS-IS administrative distance
	Configure the IS-IS route summary
	Configure the maximum number of load-balanced routes for the IS-IS
	Configure the IS-IS inter-layer route leakage
	Configure the IS-IS ATT-bit
Configure the IS-IS network optimization	Configure the IS-IS interface priority
	Configure the IS-IS passive interface
	Configure the IS-IS Hello packet parameter
	Configure the IS-IS LSP packet parameter
	Configure the IS-IS SNP packet parameter
	Configure the IS-IS SPF calculation interval
	Configure the maximum number of areas for the IS-IS
	Configure the IS-IS host name mapping

Configuration Task	
	Configure the IS-IS interface to be added to the mesh group
Configure the IS-IS network authentication	Configure the IS-IS neighboring authentication
	Configure the IS-IS route authentication
Configure the IS-IS to coordinate with the BFD	Configure the IS-IS to coordinate with the BFD
Configure IS-IS GR	Configure IS-IS GR

6.9.2.1 Configure IS-IS Basic Function

Configuration Condition

Before using the IS-IS protocol, first complete the following tasks:

- Configure the link layer protocol to ensure the normal communication at the link layer.
- Configure the network layer IP address of the interface to enable the neighboring nodes to be reachable at the network layer.

Enable IS-IS Protocol

Multiple IS-IS processes can operate at the same time in the system. Each process is identified by different process names.

Table 652 Enable the IS-IS protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Create the IS-IS process and enter the IS-IS configuration mode	router isis [*area-tag*]	Mandatory By default, the IS-IS process does not operate in the system. The process name is *area-tag*.
Configure the network entity title for the IS-IS	net *entry-title*	Mandatory By default, the network entity title is not configured for the IS-IS.
Return to the global configuration mode	exit	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the IS-IS protocol on the interface	ip router isis [*area-tag*]	Mandatory By default, the IS-IS protocol is not enabled on the interface.

Note

- The IS-IS protocol cannot operate without the network entity title.

Configure IS-IS VRF Attribute

Multiple IS-IS processes can exist in the same VRF, but only one IS-IS process with Level-2 attribute in the VRF.

Table 653Configure the IS-IS VRF attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-

Step	Command	Description
Enter the VRF attribute for the IS-IS	vrf *vrf-name*	Optional By default, the IS-IS process locates at the global VRF.

6.9.2.2 Configure IS-IS Layer Attribute

Configuration Condition

Before configuring the IS-IS layer attribute, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Layer Attribute

The IS-IS layer attribute is divided into the global layer attribute and the interface layer attribute. The global layer attribute is the IS-IS intermediate system, which is further classified into the following three types:

- Level-1 intermediate system: Only the link status database of Level-1 is available and only the routing in the Level-1 area can be advertized and learnt.
- Level-2 intermediate system: Only the link status database of Level-2 is available and only the routing in the Level-2 area can be advertized and learnt.
- Level-1-2 intermediate system: Both the link status database of Level-1 and Level-2 are available and both the routing in the Level-1 and Level-2 area can be advertized and learnt. The Level-1-2 intermediate system is the interconnection device in the Level-1 and Level-2 area.

The layer attribute of the IS-IS interface is classified into the following three

types:

- Level-1 attribute interface: Only the Level-1 packet of the IS-IS protocol can be transmitted and received and only the neighbor of Level-1 can be established.
- Level-2 attribute interface: Only the Level-2 packet of the IS-IS protocol can be transmitted and received and only the neighbor of Level-2 can be established.
- Level-1-2 attribute interface: Both the Level-1 packet and Level-2 packet of the IS-IS protocol can be transmitted and received and both the neighbors of Level-1 and Level-2 can be established.

The IS-IS interface layer attribute depends on the IS-IS global layer attribute. The Level-1 intermediate system only has the interface of Level-1 attribute, the Level-2 intermediate system only has the interface of Level-2 attribute, and the Level-1-2 intermediate system can has interfaces of all attributes.

Table 654 Configure the IS-IS global layer attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS global layer attribute	is-type { level-1 | level-1-2 | level-2-only }	Optional By default, the IS-IS global layer attribute is Level-1-2.

Table 655 Configure the IS-IS interface layer attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the interface layer attribute	isis circuit-type [level-1 | level-1-2 | level-2]	Optional By default, the interface layer attribute is consistent with the global layer attribute when the interface layer attribute is not specified.

6.9.2.3 Configure IS-IS Route Generation

Configuration Condition

Before configuring the IS-IS route generation, first complete the following tasks:

- Configure the IP address for the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Default Route

The Level-2 area of the IS-IS protocol cannot generate the default route during operating. You can configure to add a default route with the destination IP address as 0.0.0.0/0 in the Level-2 LSP and release it. When other areas of the same level in the intermediate system receive the route information, a default route will be added in the route table.

Table 656Configure the IS-IS default route

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the IS-IS to release he default route	default-information originate	Mandatory By default, the default route is not released.

Configure IS-IS Routing Redistribution

The routing redistribution can be used to introduce the routing information of other routing protocols to the IS-IS protocol. This enables the interconnection between the autonomous system of the IS-IS protocol and the autonomous system of other routing protocols or the routing area. When the external routing is introduced, the routing introduction policy and the routing layer attribute after introduction are specified.

Table 657Configure the IS-IS routing redistribution

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-

Step	Command	Description
Configure the IS-IS routing redistribution	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*]	Mandatory By default, information of other routing protocols are not redistributed.

6.9.2.4 Configure S-IS Routing Control

Configuration Condition

Before configuring the IS-IS routing feature, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Metric Style

Initially, the IS-IS only has the narrow metric style. When the narrow metric style is used, the maximum metric value is 63. With the expansion of the network scale, the metric style cannot satisfy the requirements. Therefore, the wide metric style emerges whose metric value can reach 16777214. Devices use different metric styles cannot advertise and learn the routing information from each other. To realize the transition between the two metric styles, the configuration method for the transition metric style is provided.

The wide metric style is recommended.

Table 658Configure the IS-IS metric style

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
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

When the IS-IS protocol is enabled on the interface, the IS-IS routing metric is the global metric value. The following command can be used to specify a metric value for each interface.

Table 659 Configure the interface metric value

Step	Command	Description
Enter the 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.
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

Step	Command	Description
		value is used.

Configure IS-IS Administrative Distance

The system chooses the primary routing based on the administrative distance. The smaller the administrative distance is, the higher priority the routing has.

Table 660 Configure the IS-IS administrative distance

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the IS-IS routing administrative distance	distance *distance-value*	Optional By default, the administrative distance is 115.

Configure IS-IS Route Summary

The route summary summarizes multiple pieces of routing information as a piece of routing information. After the route summary is configured for the IS-IS, the number of advertisements to the subnet reduces effectively and the link status database and route table size reduce. This effectively saves the memory and CPU resources. This configuration is generally applied to the Level-1-2 edge device, reducing the routing information of layer advertisement.

Table 661 Configure the IS-IS route summary

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the 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]	Mandatory By default, the route summary is not performed.

Configure the maximum number of load-balanced routes for the IS-IS

There are multiple paths of the same cost to the same destination IP address. These ECMP (equal cost multipath routing) can improve the link utilization rate. The user can control the maximum number of the IS-IS ECMPs.

Table 662 Configure the maximum number of load-balanced routes for the IS-IS

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the maximum number of load-balanced routes	maximum-paths *max-number*	Optional By default, the maximum

Step	Command	Description
for the IS-IS		number of paths for load balancing is 4.

Configure IS-IS Inter-layer Route Leakage

By default, the IS-IS only leak the Level-1 routing to the Level-2, but the Level-1 area cannot know the routing of the Level-2 area. The inter-layer route leakage can be configured to introduce the Level-2 routing to the Level-1 area. When configuring the inter-layer route leakage, the routing policy can be specified to only leak the route that matches the condition.

Table 663 Configure the IS-IS inter-layer route leakage

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the route leakage between the IS-IS layer	propagate { level-1 into level-2 | level-2 into level-1 } [distribute-list *access-list-name* | route-map *route-map-name*]	Mandatory By default, the Level-1 leaks its route to the Level-2.

Configure IS-IS ATT-bit

In the Level-1-2 device, the ATT-bit is used to inform other nodes whether this node has the connection to other areas. If yes, the ATT-bit will be set to 1 automatically

and other nodes will generate a default route to this node. This increases the service load of this node. To avoid this situation, the ATT-bit can be forcibly set to 0.

Table 664 Configure the IS-IS ATT-bit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the IS-IS ATT-bit	set-attached-bit { on | off }	Mandatory By default, the ATT-bit is set based on whether the node is connected to other areas.

6.9.2.5 Configure IS-IS Network Optimization

Configuration Condition

Before configuring the IS-IS adjustment and optimization, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Interface Priority

The IS-IS chooses a node on the broadcast link as the DIS node. The DIS node sends the CSNP packet periodically to synchronize the link status database on the entire network. The Level-1 and Level-2 select the DIS node respectively. The interface with the highest priority is selected as the DIS node. The node with the large MAC address

is selected as the DIS node for the nodes with the same priority.

Table 665Configure the IS-IS interface priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IS-IS interface priority	isis priority *priority-value* [level-1 | level-2]	Optional By default, the interface priority is 64.

Configure IS-IS Passive Interface

The passive interface does not receive and transmit the IS-IS protocol packet, but still releases the directly connected network routing information of this interface. The IS-IS can reduce the bandwidth and CPU handling time through configuring the passive interface. Based on this configuration, the IS-IS can be specified to only release the directly connected network routing information of the passive interfaces and not release the directly connected network routing information of the non-passive interfaces.

Table 666Configure the IS-IS passive interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS passive	passive-interface *interface-*	Mandatory

Step	Command	Description
interface	*name*	By default, the IS-IS does not have the passive interface.
Configure the IS-IS only to release the routing information of the passive interface	advertise-passive-only	Optional By default, the directly connected network routing information of the interface enabled with the IS-IS protocol is released.

Configure IS-IS Hello Packet Parameter

1. Configure the Hello packet delivery interval.

The interface enabled with the IS-IS protocol will send the Hello packet to keep the neighboring relationship with the neighboring devices. The smaller delivery interval of the Hello packet is, the faster the network convergence is. However, more bandwidth will be occupied.

Table 667 Configure delivery interval for the Hello packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the Hello packet delivery interval on the interface	isis hello-interval { *interval* | minimal } [level-1 | level-2]	Optional By default, the delivery interval of the Hello packet is 10s.

2. Configure the number of invalid Hello packets.

The IS-IS calculates the neighbor relationship retention time based on the number of invalid Hello packets and informs the retention time to the neighboring device. If

the neighboring device does not receive the Hello packet from this device during this period, the neighbor relationship is invalid and the routing calculation will be recalculated.

Table 668 Configure the number of invalid Hello packets

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the number of invalid Hello packets on the interface	isis hello-multiplier *multiplier* [level-1 | level-2]	Optional By default, the number of invalid Hello packets is 3.

3. Configure to cancel the Hello packet padding function.

If MTU values on the interface at both sides of the link are inconsistent, as a result, smaller packets can be transmitted but larger packets cannot be transmitted. To avoid such situation, the IS-IS adopts the padding Hello packet to the interface MTU value to make the neighbor relationship cannot be established. However, this method wastes the bandwidth. In actual network, there is no need to configure the padding Hello packet. Only the small Hello packets are transmitted.

Table 669 Configure to cancel the Hello packet padding function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Cancel the Hello packet padding function	no isis hello padding	Mandatory By default, the Hello packet padding function is enabled.

Configure IS-IS LSP Packet Parameter

4. Configure the maximum survival time for the LSP packet.

Each LSP packet has a maximum survival time. When the survival time of the LSP packet reduces to 0, the LSP packet will be deleted from the link status database. The maximum survival time of the LSP packet must be larger than the LSP packet refresh interval.

Table 670Configure the IS-IS LSP packet parameter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the maximum survival time for the LSP packet	max-lsp-lifetime *life-time*	Optional By default, the maximum survival time of the LSP is 1200s.

5. Configure the LSP packet refresh interval.

The IS-IS protocol advertises and learns the routing through interacting each LSP packets. The nodes save the received LSP packets in the link status database. Each LSP packet has a maximum survival time and each node needs to refresh its LSP packet periodically to prevent the LSP packet maximum survival time reducing to 0 and keep the LSP packet in the entire area synchronization. Reducing the LSP packet delivery interval can accelerate the network convergence speed, but will occupy more bandwidth.

Table 671 Configure the LSP packet update packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the LSP packet refresh interval	lsp-refresh-interval *refresh-interval*	Optional By default, the packet refresh interval for the periodical packet delivery is 900s.

6. Configure the LSP packet generation interval.

Periodical refresh will generate new LSP packet. Besides, the interface status changes and network status changes will also trigger new LSP packet generation. To prevent frequently generated LSP packets occupying too much CPU resources, the user can configure the minimum LSP packet generation interval.

Table 672 Configure the LSP packet generation interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the LSP packet generation interval	lsp-gen-interval [level-1 | level-2] *max-interval* [*initial-interval* [*secondary-interval*]]	Optional By default, the LSP packet generation interval is 50 ms.

7. Configure the LSP packet delivery interval.

Every generated LSP packet will be delivered on the interface. To avoid frequently generated LSP packet will greatly occupy the interface bandwidth. Each interface is configured with the minimum delivery interval of the LSP packet.

Table 673 Configure the LSP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the LSP packet delivery interval	isis lsp-interval *min-interval*	Optional By default, the delivery interval of the LSP packet is 33 ms.

8. Configure the LSP packet retransmission time.

On the point-to-point link, the IS-IS sends the LSP packet and the then requires the peer end to send the PSNP acknowledgement message. If the IS-IS does not receive the acknowledgement message, the IS-IS will send the LSP packet again. The time waiting the acknowledgement message is the LSP packet retransmission interval. The retransmission interval can be set as required by the user to avoid LSP packet retransmission when the acknowledgement message is not received due to large delay.

Table 674Configure the LSP packet retransmission time

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the LSP packet retransmission time	isis retransmit-interval *interval* [level-1 | level-2]	By default, the retransmission time is 5s.

9. Configure the LSP MTU value.

The IS-IS protocol packet cannot perform automatic fragmentation. In order not to affecting normal LSP packet spread, the maximum length of the LSP packet in a

routing domain cannot exceed the minimum MTU value on the IS-IS interfaces of all devices. Therefore, when the interface MTU values are inconsistent on devices in the routing domain, it is recommended that the maximum length of the LSP packet is set uniformly.

Table 675 Configure the LSP MTU value

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the LSP packet MTU value	lsp-mtu *mtu-size* [level-1 | level-2]	Optional By default, the MTU value of the LSP packet is 1492 bytes.

Configure IS-IS SNP Packet Parameter

10.Configure the CSNP packet delivery interval.

The selected nodes on the broadcast link need to send the CSNP packet periodically to synchronize the link status database on the entire network. The CSNP packet delivery interval is adjusted based on the actual situation.

Table 676Configure the CSNP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the CSNP packet delivery interval	isis csnp-interval *interval* [level-1 | level-2]	Optional By default, the CSNP packet

Step	Command	Description
		delivery interval is 10s.

11.Configure the PSNP packet delivery interval

On the broadcast link, the PSNP packet synchronizes the link status database on the entire network. On the point-to-point link, the PSNP packet confirms the received LSP packet. To avoid a large number of PSNP packets being delivered over the interface. A minimum delivery interval is set for the PSNP packet and the user can change the interval dynamically. The PSNP packet delivery interval cannot be set to a too large value. If the packet delivery interval is set to a too large value, the link status database synchronization on the entire network will be affected for the broadcast link, and the LSP packet may be redelivered caused by not timely receiving the acknowledgment message for the point-to-point link.

Table 677 Configure the PSNP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the PSNP packet delivery interval	isis psnp-interval *min-interval* [level-1 | level-2]	Optional By default, the PSNP packet delivery interval is 2s.

Configure IS-IS SPF Calculation Interval

The IS-IS link status database changes will trigger the SPF routing calculation. Frequent SPF calculation will consume a mass of CPU resources and user can

configure the SPF calculation interval.

Table 678Configure the IS-IS SPF calculation interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure the IS-IS SPF calculation interval	spf-interval [level-1 | level-2] *maximum-interval* [*min-initial-delay* [*min-second-delay*]]	Optional

Configure Maximum Number of Areas for IS-IS

Multiple area IP addresses can be configured in an IS-IS process. Multiple area IP addresses are mainly applied in the following two situations that multiple Level-1 areas are combined as a Level-1 area, or a Level-1 area is divided into multiple Level-1 areas.

Table 679 Configure the maximum number of areas for the IS-IS

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the maximum number of areas for the IS-IS	max-area-addresses *max-number*	Optional By default, the maximum number of the area IP addresses is 3.

Note

- This configuration must be consistent in the entire IS-IS Level-1 routing domain. Otherwise, the Level-1 neighbor cannot be established normally. The Level-2 neighbor is not affected.

Configure IS-IS Host Name Mapping

The IS-IS uniquely identifies a intermediate system using the system ID with a fixed length of 6 bytes. When viewing the system information such as the neighbor relationship and link status database, the system ID cannot enable the user to visually associate the system ID with the host name. The IS-IS supports the mapping between the system ID and the host name to enable the user to view the system information more visually and conveniently. The IS-IS host name mapping can be configured in the following two methods:

12.Configure the IS-IS static host name mapping.

The IS-IS static host name mapping is manually established by the user between the system ID and the host name for the remote device .

Table 680 Configure the IS-IS static host name mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS static hostname mapping	hostname static *system-id host-name*	Mandatory

13.Configure the IS-IS dynamic host name mapping.

The static host name mapping requires the user to configure the system ID and host name mapping of other devices on each device in the network, which has a heavy

workload. The dynamic host name mapping only configures the host name for each device, and other devices in the network can learn the host name of the device when the host name advertisement function is enabled.

Table 681 Configure the IS-IS dynamic host name mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS dynamic host name mapping	hostname dynamic { *host-name* | area-tag | recv-only | system-name }	Mandatory By default, only the host names advertized by other devices are learnt.

Configure IS-IS Interface to Be Added to Mesh Group

When the IS-IS interface is not added to the mesh group, the LSP packet received from an interface will be sent out on all the other IS-IS interfaces. This results in great bandwidth waste in a full mesh connected network. To avoid this situation, several IS-IS interfaces can be added to a mesh group. When an interface receives the LSP packet, it only sends the LSP packet out to the interface that is not in the same mesh group with this interface.

Table 682Configure the IS-IS interface to be added to the mesh group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface interface-name	-

Step	Command	Description
Configure the IS-IS interface to be added to the mesh group	isis mesh-group { group-number | blocked }	Mandatory By default, the IS-IS interface is not added to the mesh group.

Note

- The **isis mesh-group blocked** command can be used to configure the interface as the obstructive interface. The obstructive interface will not send the LSP packet actively and only send the LSP packet when receives the LSP request.

6.9.2.6 Configure IS-IS Network Authentication

Configuration Condition

Before configuring the IS-IS network authentication, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Neighboring Authentication

When the neighbor relationship authentication is enabled for the IS-IS, the authentication information will be added to the delivered Hello packet and the received Hello packet will be authenticated. If the authentication fails, the neighbor relationship will not be established. This can prevent the neighbor relationship being established with the unreliable devices.

Table 683Configure the IS-IS neighboring authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the Hello packet authentication mode	isis authentication mode { md5 | sm3 | text } [level-1 | level-2]	Mandatory By default, the authentication function is not enabled.
Configure the Hello packet authentication password	isis authentication key { 0 | 7 } *password* [level-1 | level-2]	Either By default, the authentication password is not configured. The authentication password can be configured using the password chain. For details about the password chain configuration, refer to the password chain configuration chapter in the configuration manual.
	isis authentication key-chain *key-chain-name* [level-1 | level-2]	

Configure IS-IS Route Authentication

When the routing information authentication is enabled for the IS-IS, the authentication information will be added to the LSP and SNP packets and the received LSP and SNP packets will be authenticated. If the authentication fails, the packet will be dropped directly. This can prevent the unreliable routing information spreading to the IS-IS network.

Table 684Configure the IS-IS route authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the authentication mode of the routing information packet	authentication mode { md5 | sm3 | text } [level-1 | level-2]	Mandatory By default, the authentication function is not enabled.
Configure the authentication password of the routing information packet	authentication key { 0 | 7 } *password* [level-1 | level-2]	Either By default, the authentication password is not configured. The authentication password can be configured using the password chain. For details about the password chain configuration, refer to the password chain configuration chapter in the configuration manual.
	authentication key-chain *key-chain-name* [level-1 | level-2]	

6.9.2.7 Configure IS-IS to Coordinate with the BFD

The IS-IS to coordinate with the BFD is configure to fast detect the link faults and enable the backup link for communication. The IS-IS to coordinate with the BFD can be configured in the following two methods: All interfaces enabled with the IS-IS protocol are coordinated with the BFD and the interface is specified to coordinate with the BFD.

For details about the BFD parameter information, refer to the BFD configuration manual.

Configuration Condition

Before configuring the IS-IS to coordinate with the BFD, first complete the

following task:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS to Coordinate with BFD

Table 685 Configure the IS-IS to coordinate with the BFD

Step	Command
Enter the global configuration mode	configure terminal
Enter the interface configuration mode	interface *interface-name*
Configure the interface to enable the BFD link detection function	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 the BFD link detection function	bfd all-interfaces

6.9.2.8 Configure IS-IS Fast Re-routing

Configuration Condition

Before configuring IS-IS fast re-routing, ensure that:

- Interface IP addresses have been configured so that neighbor nodes are reachable at the network layer.
- Enable the IS-IS protocol.

Configure IS-IS Fast Re-routing

In the IS-IS network, if the link or device fails, the packet passing the fault point will be dropped or generate the loop and the caused traffic interruption will not recover until the protocol re-converges, which often lasts for several seconds. To reduce the

traffic interruption time, you can configure the IS-IS fast re-routing. Apply the route map to set the backup next hop for the matched route. Once the active link fails, the traffic passing the faulty link will switch to the standby link at once.

Table 686 Configure the IS-IS fast re-routing

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the IS-IS configuration mode.	router isis [*area-tag*]	-
Enter the IS-IS IPv4 address family configuration mode	address-family ipv4 unicast	-
Configure ISIS to enable the fast re-routing function	fast-reroute route-map *route-map-name*	Mandatory By default, do not enable the IS-IS fast re-routing function.
Configure IS-IS to enable the dynamic fast re-routing function	fast-reroute loop-free-alternate [route-map *route-map-name*]	Mandatory By default, do not enable the IS-IS dynamic fast re-routing function.
Configure IS-IS to enable the pic function	pic	Mandatory After enabling the pic function, enable the auto fast re-routing function. By default, do not enable the IS-IS pic function.

Note

- The IS-IS fast reroute function is divided into static fast reroute and dynamic fast reroute.
- The static fast rerouting function needs to associate with the route-map, and set the next hop interface and address of the backup route in the route-map.
- At present, dynamic fast reroute only supports point-to-point network, that is, the network type of all outgoing interfaces of the device needs to be point-to-point. After configuring dynamic fast reroute, the device automatically calculates and sets the backup next hop interface and address. Dynamic fast rerouting can also be associated with route-map. Only the routes matching route map are set to back up the next hop interface and address.
- The various modes of enabling rerouting are mutually exclusive;

6.9.2.9 Configure IS-IS GR

GR (Graceful Restart) is used to keep the route information of the forwarding layer of the local device and the neighbor device unchanged during the active/standby switchover, not affecting the forwarding. After switching the device and running again, the protocol layer of the two devices synchronizes the route information and updates the forwarding layer, so as to keep the data forwarding un-interrupted during the device switchover.

There are two roles in the GR process:

- GR Restarter: the device performing the protocol graceful restart
- GR Helper: the device helping the protocol graceful restart

The distributed device can act as GR Restarter and GR Helper, while the centralized device can only act as GR Helper, helping Restarter to complete GR.

Configuration Condition

Before configuring IS-IS GR, first complete the following task:

- Configure the IP address of the interface, making the neighboring node network layer reachable
- Enable the IS-IS protocol

Configure IS-IS GR Restarter

Table 687 Configure IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure IS-IS to enable the GR function	nsf ietf	Mandatory By default, do not enable the GR function.
Configure the times of re-transmitting the message of advertising to enter the GR process	nsf interface-expire *resend-cnt*	Optional By default, the re-transmission times is 3.
Configure the wait time of entering the re-transmission of the message for entering the GR process	nsf interface-timer *wait-time*	Optional By default, the wait time is 10s.

Configure IS-IS GR Helper

GR Helper helps Restarter to complete GR. By default, the device enables the function and the user can disable the function via the command.

Table 688 Configure IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS GR Helper not to have the Helper capability	nsf ietfhelper-disable	Mandatory Configure the IS-IS GR Helper not to have the Helper capability

6.9.2.10 IS-IS Monitoring and Maintaining

Table 689 The IS-IS monitoring and maintaining

Command	Description
clear isis [instance -null | *area-tag*] statistics [*interface_name*]	Clear the statistics information of the IS-IS protocol operation
clear isis [instance -null | *area-tag*] process	Restart the IS-IS protocol process
show isis [instance -null | *area-tag*]	Display the IS-IS process information
show isis instance { -null | *area-tag* } ipv4 bfd-sessions	Display the BFD session information of the IS-IS process
show isis [instance -null | *area-tag*] database [*lsp_id*] [detail] [l1 / l2] [level-1 / level-2] [self] [verbose]	Display the IS-IS link status database information
show isis interface [*interface-name*] [detail]	Display the information of the IS-IS protocol interface operation
show isis [instance –null | *area-tag*] ipv4 reach-info	Display the IS-IS IPv4 subnet reachable information
show isis [instance –null | *area-tag*] ipv4 route	Display the IS-IS IPv4 routing information

Command	Description
show isis [instance –null | *area-tag*] ipv4 topology	Display the IS-IS IPv4 topology information
show isis [instance – null | *area-tag*] is-reach-info [level-1 | level-2]	Display the IS-IS adjacent node information
show isis [instance –null | *area-tag*] mesh-groups	Display the IS-IS mesh group
show isis [instance –null | *area-tag*] neighbors [*interface-name*] [detail]	Display the IS-IS neighbor information
show isis [instance –null | *area-tag*] statistics [*interface-name*]	Display the statistics information of the IS-IS protocol operation
show isis router	Display the IS-IS host name information

6.9.3 IS-IS Typical Configuration Example

6.9.3.1 Configure IS-IS Basic Function

Network Requirements

- Configure the IS-IS protocol to realize the network interconnection between devices.
- Device1 is the Level-1 router and Device2 is the Level-1-2 router. Device1 and Device2 are in the same area, Area 10. Device3 is the Level-2 router in Area 20. Device2 connects the two areas.

Network Topology

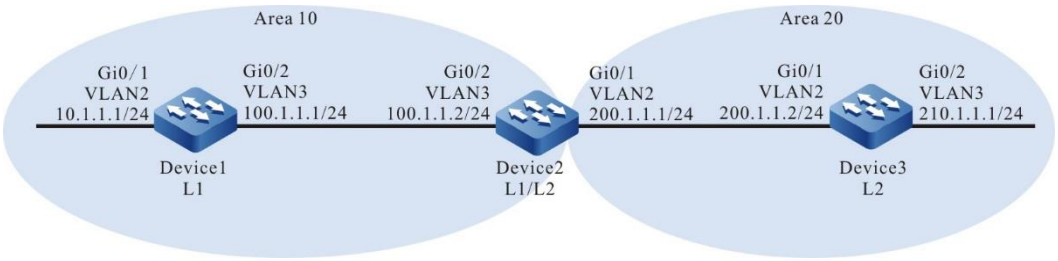


Figure 136 Networking of configuring the IS-IS basic functions

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device2.

```
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
```

#Configure the IS-IS process as 100, area number as 20, and type as Level-2 and enable the process on the interface on Device3.

```
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.

#View the IS-IS neighboring 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
```

#View the IS-IS neighboring information on 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 builds the IS-IS neighbor with Device1 and Device3, respectively.

#View the IS-IS neighboring 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
```

#View the routing information of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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, 16:56:18, vlan2
C   100.1.1.0/24 is directly connected, 18:37:57, vlan3
C   127.0.0.0/8 is directly connected, 284:02:13, 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
```

A default routing is in the route table of Device1 and the next hop is Device2.

#View the routing information of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

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, 18:39:58, vlan3
C   127.0.0.0/8 is directly connected, 20:16:34, lo0
C   200.1.1.0/24 is directly connected, 18:39:37, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, 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 Level-1 and Level-2 routing.

#View the routing information of Device3.

```
Device3#show ip 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, E - IRMP, EX - IRMP external

i   10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i   100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C   127.0.0.0/8 is directly connected, 945:29:12, lo0
C   200.1.1.0/24 is directly connected, 18:40:27, vlan2
C   210.1.1.0/24 is directly connected, 16:59:04, 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 the Level-1 routing and the Level-1 leaks the routing to Level-2 by default.

Note

- The metric type is the narrow metric by default. The wide metric is recommended.
- The IS-IS entity attribute is Level-1-2 by default.

6.9.3.2 Configure IS-IS DIS Node Selection

Network Requirements

- Specify the device as the DIS node by changing the priority.

- Device1 and Device2 are the Level-1-2 devices, Device3 is the Level-1 device, and Device4 is the Level-2 device. Device1, Device2, Device3, and Device4 are in the same broadcast network and in the same area, Area 10.

Network Topology

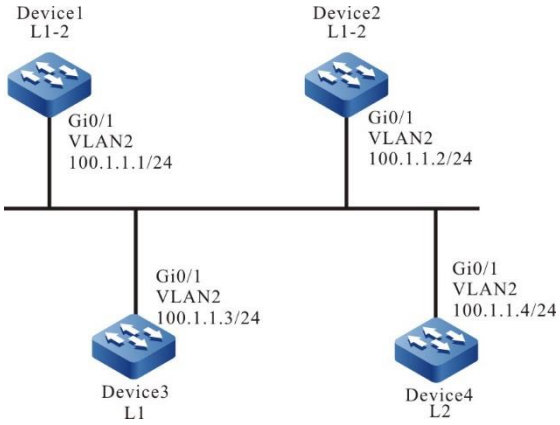


Figure 137 Networking of configuring the IS-IS DIS selection

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device2.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface on Device3.

```
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
```

#Configure the IS-IS process as 100, area number as 20, and type as Level-2 and enable the process on the interface on Device4.

```
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
```

#View the IS-IS neighboring 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 the DIS node of Level-1. The pseudo node of Level-2 is 0000.0000.0004.01 and Device1 is the DIS node of Level-2.

#Run the **show isis interface** command to view the MAC address of the interface. In the default priority, the DIS node is selected based on the principle that a larger MAC address of the physical interface has a higher 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.

#View the IS-IS neighboring 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 the DIS node of Levev-1-2.

Note

- The IS-IS interface priority is 64 by default.

6.9.3.3 Configure IS-IS Inter-layer Route Leakage

Network Requirements

- Configure the inter-layer leakage on the Level-1-2 to leak the routing of Level-2 to Level-1.

- Device1 is a Level-1 router and Device2 is a Level-1-2 router. Device1 and Device2 are in the same area and the area number is 10. Device3 is a Level-2 router with an area number of 20. Device2 is responsible for connecting two areas.

Network Topology

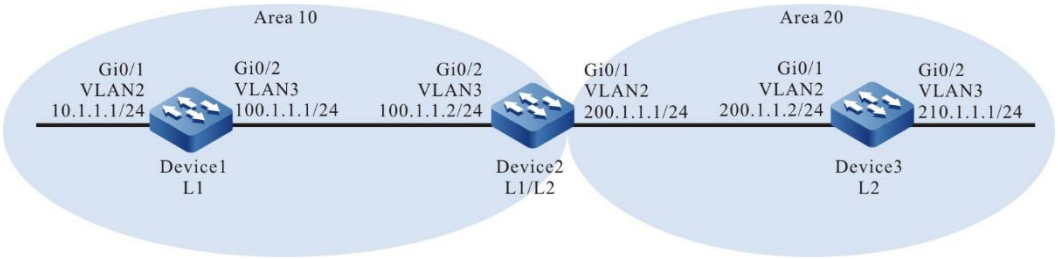


Figure 138 Networking of configuring the IS-IS inter-layer leakage

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device2.

```
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
```

#Configure the IS-IS process as 100, area number as 20, and type as Level-2 and enable the process on the interface on Device3.

```
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
```

#View the routing information of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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, 16:56:18, vlan2
C   100.1.1.0/24 is directly connected, 18:37:57, vlan3
C   127.0.0.0/8 is directly connected, 284:02:13, 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
```

A default routing is in the route table and the next hop is Device2. No Level-2 routing advertised by Device3 is in the route table.

#View the routing information of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

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, 18:39:58, vlan3
C   127.0.0.0/8 is directly connected, 20:16:34, lo0
C   200.1.1.0/24 is directly connected, 18:39:37, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, 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 Level-1 and Level-2 routing.

#View the routing information of Device3 and Device3 contains the Level-1 routing advertised by Device1.

```
Device3#show ip 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, E - IRMP, EX - IRMP external

i   10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i   100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C   127.0.0.0/8 is directly connected, 945:29:12, lo0
C   200.1.1.0/24 is directly connected, 18:40:27, vlan2
C   210.1.1.0/24 is directly connected, 16:59:04, 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-layer leakage.

#Configure the inter-layer leakage for Device2.

```
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.

#View the routing information of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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, 16:56:18, vlan2
C   100.1.1.0/24 is directly connected, 18:37:57, vlan3
C   127.0.0.0/8 is directly connected, 284:02:13, 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, 00:00:01, 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
```

Besides the default routing, Device1 also learns the Level-2 routing advertised by Device3.

6.9.3.4 Configure IS-IS Routing Redistribution

Network Requirements

- Configure the redistribution to introduce the external routing to the IS-IS, enabling network interconnection between devices.
- Device1 and Device2 are the Level-2 routers. Configure the IS-IS and the Area 10. Configure the OSPF on Device2 and Device3. Redistribute the OSPF routing to the IS-IS through the configuration on Device2.

Network Topology

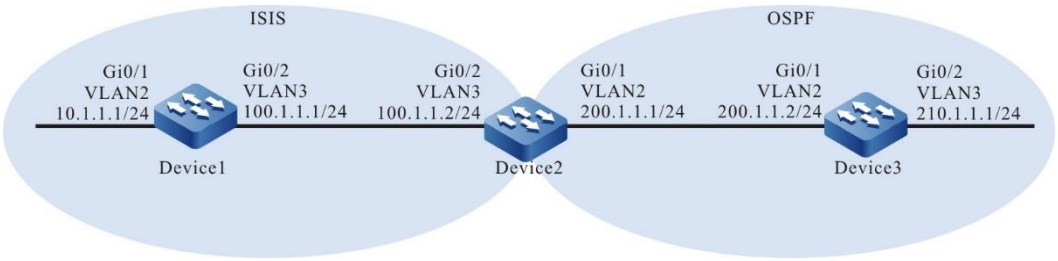


Figure 139 Networking of configuring the IS-IS routing redistribution

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device2.

```
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 the 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
```

#View the route table of Device1. Device1 does not learn the OSPF routing redistributed by Device2.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 00:58:39, vlan2
C   100.1.1.0/24 is directly connected, 06:55:35, vlan3
C   127.0.0.0/8 is directly connected, 603:06:22, 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
```

#View the route table of Device2. Device2 learns the IS-IS and OSPF routing.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

i   10.1.1.0/24 [115/20] via 100.1.1.1, 15:45:37, vlan3
C   100.1.1.0/24 is directly connected, 22:38:58, vlan3
C   127.0.0.0/8 is directly connected, 300:03:03, lo0
C   200.1.1.0/24 is directly connected, 22:38:58, vlan2
O   210.1.1.1/32 [110/2] via 200.1.1.2, 15:43:35, 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 the IS-IS to redistribute the OSPF routing..

#Configure the OSPF routing to be redistributed to IS-IS Level-2 on Device2.

```
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.

#View the routing information of Device1. Device1 leans the OSPF routing redistributed by Device2.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 16:47:30, vlan2
C   100.1.1.0/24 is directly connected, 22:44:27, 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, 00:00:05, vlan3
i   210.1.1.1/32 [115/10] via 100.1.1.2, 00:00:05, 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 redistributed OSPF routing.

6.9.3.5 Configure IS-IS Neighboring Authentication

Network Requirements

- Enable the authentication on the interface to enable the devices configured with the same password establishing the neighbor relationship.
- Device1 is the Level-1 router, Device2 is the Level-1-2 router, and Device1 and Device2 are in the same area, Area 10. Device3 is the Level-2 router in Area 20. Device2 connects the two areas.

Network Topology

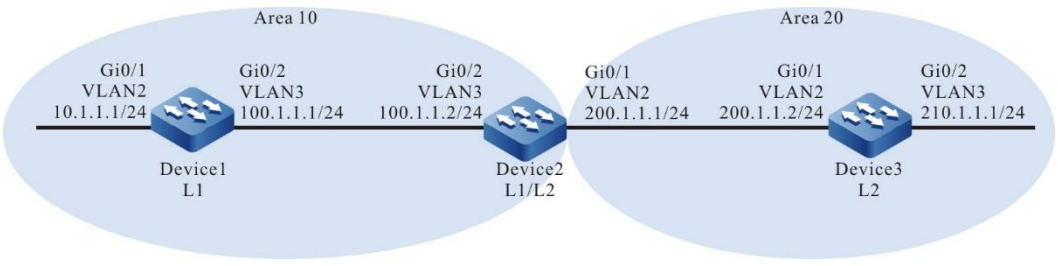


Figure 140 Networking of configuring the IS-IS neighbor authentication

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface on Device2.

```
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
```

#Configure the IS-IS process as 100, area number as 20, and type as Level-2 and enable the process on the interface on Device3.

```
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
```

#View the IS-IS neighboring 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
```

#View the IS-IS neighboring information on 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
```

#View the IS-IS neighboring 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 the authentication.

#Configure the MD5 authentication and password admin on the interface of Device2.

```
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
```

#View 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
```

At this time, Device1 and Device3 are not configured with the authentication.

Device2 does not establish the IS-IS neighbor.

#Configure the MD5 authentication and password admin on the VLAN3 interface of Device1.

```
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
```

#Configure the MD5 authentication and password admin on the VLAN2 interface of Device3.

```
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.

#View the IS-IS neighboring 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
```

It can be observed that the IS-IS neighbor is successfully established between Device1 and Device2. It indicates that the authentication succeeds.

#View the IS-IS neighboring information on 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
```

It can be observed that the IS-IS neighbor is successfully established between Device2 and Device1/Device3. It indicates that the authentication succeeds.

#View the IS-IS neighboring 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
```

It can be observed that the IS-IS neighbor is successfully established between Device3 and Device2. It indicates that the authentication succeeds.

#View the routing information of Device2. Device2 can normally receives the routing advertised by Device1 and Device3.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

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, 18:39:58, vlan3
C   127.0.0.0/8 is directly connected, 20:16:34, lo0
C   200.1.1.0/24 is directly connected, 18:39:37, vlan2
i   210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, 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
```

6.9.3.6 Configure IS-IS to Coordinate with BFD

Network Requirements

- Configure the BFD coordination between devices. When the main line is faulty, services can be quickly switched to the backup line.
- Device1, Device2, and Device3 are the Level-2 routers in the same area, Area 10. Configure the BFD on Device1 and Device3 to initiate a session. When the line between Device1 and Device3 disconnects, Device1 can perform switching quickly and learn the 10.1.1.1/24 routing from Device2.

Network Topology

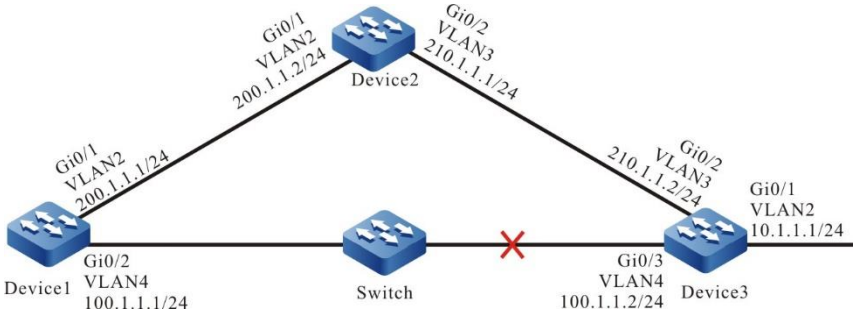


Figure 141 Networking of configuring the IS-IS coordinating with the BFD

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IS-IS and enable the process on the interface.

#Configure the IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface on Device1.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface on Device2.

```
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
```

#Configure the IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface on Device3.

```
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
```

#View the routing information of Device1. Device1 preferentially chooses the routing 10.1.1.0/24 advertised by Device3.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

i   10.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
C   100.1.1.0/24 is directly connected, 00:09:15, vlan4
C   127.0.0.0/8 is directly connected, 253:58:17, lo0
C   200.1.1.0/24 is directly connected, 00:11:29, vlan2
i   210.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
                 [115/20] via 200.1.1.2, 00:00:15, 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 the BFD.

#Enable the 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 the 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
```

#View 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.

#When the line between Device1 and Device3 is faulty, the BFD quickly detects the fault and informs the fault to the IS-IS. The ISIS switches the routing to Device2 for communication. View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
i   10.1.1.0/24 [115/30] via 200.1.1.2, 00:00:14, vlan2
C   127.0.0.0/8 is directly connected, 112:55:25, lo0
C   200.1.1.0/24 is directly connected, 101:20:08, 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
```

#It can be viewed that the data flow from Device1 to the 10.1.1.0/24 network segment uses the line with Device2 to forward.

6.9.3.7 Configure ISIS Fast Re-routing

Network Requirements

- All devices configure the ISIS protocol.
- Device1 learns the ISIS route 192.168.1.1/32 from Device2 and Device3 at the same time. Device1 first uses the line with Device3 to forward the packet. Similarly, Device3 learns the ISIS route 100.1.1.1/32 from Device1 and Device2 at the same time. Device3 first uses the line with Device1 to forward the packet.
- Device1 and Device3 enable the ISIS fast re-routing. After the line between Device1 and Device3 fails, the service can switch to Device2 for communication fast.

Network Topology

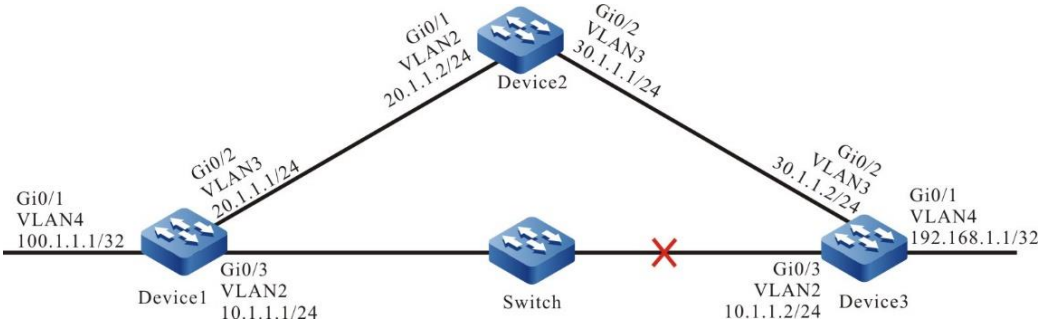


Figure 142 Configure the ISIS fast re-routing

Configuration Steps

Step 1: Configure the IP addresses of the interfaces. (Omitted)

Step 2: Configure ISIS and enable the process on the interface.

#Device1 configures the ISIS process 100, the area ID is 10, the type is Level-2, and enable the process on 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
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ip router isis 100
Device1(config-if-loopback0)#exit
```

#Device2 configures the ISIS process 100, the area ID is 10, the type is Level-2, and enable the process on 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 the ISIS process 100, the area ID is 10, the type is Level-2, and enable the process on 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 loopback 0
Device3(config-if-loopback0)#ip router isis 100
Device3(config-if-loopback0)#exit
```

Step 3: Configure the route policy.

#Configure Device1: configure route-map to call the ACL only matching 192.168.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface vlan3 and the next-hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfrr_isis
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#Configure Device3: configure route-map to call the ACL only matching 100.1.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface vlan3 and the next-hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfrr_isis
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-interface vlan3 backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure the fast re-routing.

#Configure Device1 to enable the ISIS fast re-routing.

```
Device1(config)#router isis 100
Device1(config-isis)#address-family ipv4 unicast
Device1(config-isis-af)#ipfrr route-map ipfrr_isis
Device1(config-isis-af)#exit-address-family
```

```
Device1(config-isis)#exit
```

#Configure Device3 to enable the ISIS fast re-routing.

```
Device3(config)#router isis 100
Device3(config-isis)#address-family ipv4 unicast
Device3(config-isis-af)#ipfrr route-map ipfrr_isis
Device3(config-isis-af)#exit-address-family
Device3(config-isis)#exit
```

Step 5: Check the result.

#View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.1.1.0/24 is directly connected, 00:02:39, vlan2
L   10.1.1.1/32 is directly connected, 00:02:39, vlan2
C   20.1.1.0/24 is directly connected, 06:19:51, vlan3
L   20.1.1.1/32 is directly connected, 06:19:51, vlan3
i   30.1.1.0/24 [115/20] via 20.1.1.2, 00:00:03, vlan3
                [115/20] via 10.1.1.2, 00:00:03, vlan2
C   127.0.0.0/8 is directly connected, 30:54:34, lo0
L   127.0.0.1/32 is directly connected, 30:54:34, lo0
LC  100.1.1.1/32 is directly connected, 02:54:43, loopback0
i   192.168.1.1/32 [115/20] via 10.1.1.2, 00:01:13, vlan2
```

#View the fast re-route table of Device1 and you can see that there is the route of the network 192.168.1.1/32 and the next-hop interface is vlan3.

```
Device1#show ip frr 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, E - IRMP, EX - IRMP external
i   192.168.1.1/32 [115/0] via 20.1.1.2, 00:00:03, vlan3
```

#View the backup next-hop information of Device1 and the fast re-routing backup interface is vlan3.

```
Device1#show nexthop frr detail
Index               : 262
Type                : FRR
Reference Count     : 1
Active Path         : master
```

```
Nexthop Address        : 10.1.1.2
Interface              : vlan2
Interface Vrf          : global
Channel ID             : 10
Link Header Length     : 18
Link Header            : 01017abc662b20120101010181000010800
Action                 : FORWORDING
Slot                   : 0
BK Nexthop Address     : 20.1.1.2
BK Interface           : vlan3
BK Interface Vrf       : global
BK Channel ID          : 11
BK Link Header Length  : 18
BK Link Header         : 01017a4554492012010101028100000020800
BK Action              : FORWORDING
BK Slot                : 0


Total 1 entries.
```

#After the line between Device1 and Device3 fails, the system can fast detect and switch to Device2 for communication. View the route table and fast re-route table of Device1. The egress interface to the destination network 192.168.1.1/32 in the route table is switched to the backup interface vlan3.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   10.1.1.0/24 is directly connected, 00:02:39, vlan2
L   10.1.1.1/32 is directly connected, 00:02:39, vlan2
C   20.1.1.0/24 is directly connected, 06:19:51, vlan3
L   20.1.1.1/32 is directly connected, 06:19:51, vlan3
i   30.1.1.0/24 [115/20] via 20.1.1.2, 00:00:03, vlan3
                [115/20] via 10.1.1.2, 00:00:03, vlan2
C   127.0.0.0/8 is directly connected, 30:54:34, lo0
L   127.0.0.1/32 is directly connected, 30:54:34, lo0
LC  100.1.1.1/32 is directly connected, 02:54:43, loopback0
i   192.168.1.1/32 [115/30] via 20.1.1.2, 00:01:13, vlan3
```

The processing mode of Device3 is similar with Device1.

6.10 IPv6 IS-IS

6.10.1 Overview

IPv6 IS-IS routing protocol and IS-IS routing protocol have the same behaviors except for the IP address structure in the packet. Refer to the brief introduction of IS-IS routing protocol.

6.10.2 IPv6 IS-IS Function Configuration

Table 690 IPV6 IS-IS function list

Configuration Task	
Configure the IPV6 IS-IS basic function	Enable the IPV6 IS-IS protocol
	Configure the IPV6 IS-IS VRF attribute
Configure the IPV6 IS-IS layer attribute	Configure the IPV6 IS-IS layer attribute
Configure the IPV6 IS-IS route generation	Configure the IPV6 IS-IS default route
	Configure the IPV6 IS-IS routing redistribution
Configure the IPV6 IS-IS routing control	Configure the IPV6 IS-IS metric style
	Configure the IPV6 IS-IS interface metric value
	Configure the IPV6 IS-IS administrative distance
	Configure the IPV6 IS-IS route summary
	Configure the maximum number of load-balanced routes for the IPV6 IS-IS
	Configure the IPV6 IS-IS inter-layer route leakage
	Configure the IPV6 IS-IS ATT-bit

Configuration Task	
Configure the IPV6 IS-IS network optimization	Configure the IPV6 IS-IS interface priority
	Configure the IPV6 IS-IS passive interface
	Configure the IPV6 IS-IS Hello packet parameter
	Configure the IPV6 IS-IS LSP packet parameter
	Configure the IPV6 IS-IS SNP packet parameter
	Configure the IPV6 IS-IS SPF calculation interval
	Configure the maximum number of areas for the IPV6 IS-IS
	Configure the IPV6 IS-IS host name mapping
	Configure the IPV6 IS-IS interface to be added to the mesh group
Configure the IPV6 IS-IS network authentication	Configure the IPV6 IS-IS neighboring authentication
	Configure the IPV6 IS-IS route authentication
Configure the IPV6 IS-IS GR	Configure the IPV6 IS-IS GR

6.10.2.1 Configure IPV6 IS-IS Basic Function

Configuration Condition

Before using the IPV6 IS-IS protocol, first complete the following tasks:

- Configure the link layer protocol to ensure the normal communication at the link layer.
- Configure the network layer IP address of the interface to enable the neighboring nodes to be reachable at the network layer.

Enable IPV6 IS-IS Protocol

Multiple IPV6 IS-IS processes can operate at the same time in the system. Each process is identified by different process names.

Table 691 Enable the IPV6 IS-IS protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the IPV6 IS-IS process and enter the IPV6 IS-IS configuration mode	router isis [*area-tag*]	Mandatory By default, the IPV6 IS-IS process does not operate in the system. The process name is *area-tag*.
Configure the network entity title for the IPV6 IS-IS	net *entry-title*	Mandatory By default, the network entity title is not configured for the IPV6 IS-IS.
Return to the global configuration mode	exit	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the IPV6 IS-IS protocol on the interface	ipv6 router isis [*area-tag*]	Mandatory By default, the IPV6 IS-IS

Step	Command	Description
		protocol is not enabled on the interface.

Note

- The IS-IS protocol cannot operate without the network entity title.

Configure IS-IS VRF Attribute

Table 692 Configure the IS-IS VRF attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IPV6 IS-IS configuration mode	router isis [*area-tag*]	-
Enter the VRF attribute for the IS-IS	vrf *vrf-name*	Optional By default, the IS-IS process locates at the global VRF.

6.10.2.2 Configure IPV6 IS-IS Layer Attribute

Configuration Condition

Before configuring the IPV6 IS-IS layer attribute, first complete the following tasks:

- Configure the IPv6 address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IS-IS Layer Attribute

The IS-IS layer attribute is divided into the global layer attribute and the interface layer attribute. The global layer attribute is the IS-IS intermediate system, which is further classified into the following three types:

- Level-1 intermediate system: Only the link status database of Level-1 is available and only the routing in the Level-1 area can be advertised and learnt.
- Level-2 intermediate system: Only the link status database of Level-2 is available and only the routing in the Level-2 area can be advertised and learnt.
- Level-1-2 intermediate system: Both the link status database of Level-1 and Level-2 are available and both the routing in the Level-1 and Level-2 area can be advertised and learnt. The Level-1-2 intermediate system is the interconnection device in the Level-1 and Level-2 area.

The layer attribute of the IS-IS interface is classified into the following three types:

- Level-1 attribute interface: Only the Level-1 packet of the IS-IS protocol can be transmitted and received and only the neighbor of Level-1 can be established.
- Level-2 attribute interface: Only the Level-2 packet of the IS-IS protocol can be transmitted and received and only the neighbor of Level-2 can be established.
- Level-1-2 attribute interface: Both the Level-1 packet and Level-2 packet of the IS-IS protocol can be transmitted and received and both the neighbors of Level-1 and Level-2 can be established.

The IS-IS interface layer attribute depends on the IS-IS global layer attribute. The Level-1 intermediate system only has the interface of Level-1 attribute, the Level-2

intermediate system only has the interface of Level-2 attribute, and the Level-1-2 intermediate system can has interfaces of all attributes.

Table 693 Configure the IPV6 IS-IS global layer attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS global layer attribute	is-type { level-1 | level-1-2 | level-2-only }	Optional By default, the IS-IS global layer attribute is Level-1-2.

Table 694 Configure the IS-IS interface layer attribute

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the interface layer attribute	isis circuit-type [level-1 | level-1-2 | level-2-only]	Optional By default, the interface layer attribute is consistent with the global layer attribute when the interface layer attribute is not specified.

6.10.2.3 Configure IPV6 IS-IS Route Generation

Configuration Condition

Before configuring the IPV6 IS-IS route generation, first complete the following tasks:

- Configure the IPv6 address for the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IPV6 IS-IS Default Route

The Level-2 area of the IS-IS protocol cannot generate the default route during operating. You can configure to add a default route with the destination IP address as 0.0.0.0/0 in the Level-2 LSP and release it. When other areas of the same level in the intermediate system receive the route information, a default route will be added in the routing table.

Table 695 Configure the IS-IS default route

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the IS-IS to release he default route	default-information originate	Mandatory By default, the default route is not released.

Configure IPV6 IS-IS Routing Redistribution

The routing redistribution can be used to introduce the routing information of other routing protocols to the IS-IS protocol. This enables the interconnection between the autonomous system of the IS-IS protocol and the autonomous system of other

routing protocols or the routing area. When the external routing is introduced, the routing introduction policy and the routing layer attribute after introduction are specified.

Table 696 Configure the IPV6 IS-IS routing redistribution

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the IS-IS routing redistribution	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*]	Mandatory By default, information of other routing protocols are not redistributed.

6.10.2.4 Configure IPv6 IS-IS Routing Control

Configuration Condition

Before configuring the IPV6 IS-IS routing feature, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IPV6 IS-IS Metric Style

Initially, the IS-IS only has the narrow metric style. When the narrow metric style

is used, the maximum metric value is 63. With the expansion of the network scale, the metric style cannot satisfy the requirements. Therefore, the wide metric style emerges whose metric value can reach 16777214. Devices use different metric styles cannot advertise and learn the routing information from each other. To realize the transition between the two metric styles, the configuration method for the transition metric style is provided.

The wide metric style is recommended.

Table 697Configure the IPV6 IS-IS metric style

Step	Command	Description
Enter the 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 IPV6 IS-IS Interface Metric Value

When the IS-IS protocol is enabled on the interface, the IS-IS routing metric is the global metric value. The following command can be used to specify a metric value for each interface.

Table 698 Configure the interface metric value

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
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.
Return to the global configuration mode	exit	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the interface metric value	isis ipv6 metric {*metric-value* | maximum} [level-1 | level-2]	Optional By default, the global metric value is used.

Configure IPV6 IS-IS Administrative Distance

The system chooses the primary routing based on the administrative distance. The smaller the administrative distance is, the higher priority the routing has.

Table 699 Configure the IPV6 IS-IS administrative distance

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IPV6 IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the IS-IS routing	distance *distance-value*	Optional

Step	Command	Description
administrative distance		By default, the administrative distance is 115.

Configure IPV6 IS-IS Route Summary

The route summary summarizes multiple pieces of routing information as a piece of routing information. After the route summary is configured for the IS-IS, the number of advertisements to the subnet reduces effectively and the link status database and routing table size reduce. This effectively saves the memory and CPU resources. This configuration is generally applied to the Level-1-2 edge device, reducing the routing information of layer advertisement.

Table 700 Configure the IPV6 IS-IS route summary

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the 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]	Mandatory By default, the route summary is not performed.

Configure the maximum number of load-balanced routes for the IPV6 IS-IS

There are multiple paths of the same cost to the same destination IP address. These ECMP (equal cost multipath routing) can improve the link utilization rate. The user can control the maximum number of the IS-IS ECMPs.

Table 701 Configure the maximum number of load-balanced routes for the IPV6 IS-IS

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the maximum number of load-balanced routes for the IS-IS	maximum-paths *max-number*	Optional By default, the maximum number of paths for load balancing is 4.

Configure IPV6 IS-IS Inter-layer Route Leakage

By default, the IS-IS only leak the Level-1 routing to the Level-2, but the Level-1 area cannot know the routing of the Level-2 area. The inter-layer route leakage can be configured to introduce the Level-2 routing to the Level-1 area. When configuring the inter-layer route leakage, the routing policy can be specified to only leak the route that matches the condition.

Table 702 Configure the IPV6 IS-IS inter-layer route leakage

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the route leakage between the IS-IS layer	propagate { level-1 into level-2 | level-2 into level-1 } [distribute-list *access-list-name* | route-map *route-map-name*]	Mandatory By default, the Level-1 leaks its route to the Level-2.

Configure IPV6 IS-IS ATT-bit

In the Level-1-2 device, the ATT-bit is used to inform other nodes whether this node has the connection to other areas. If yes, the ATT-bit will be set to 1 automatically and other nodes will generate a default route to this node. This increases the service load of this node. To avoid this situation, the ATT-bit can be forcibly set to 0.

Table 703 Configure the IPV6 IS-IS ATT-bit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the IS-IS ATT-bit	set-attached-bit { on | off }	Mandatory By default, the ATT-bit is set based on whether the node is

Step	Command	Description
		connected to other areas.

6.10.2.5 Configure IPV6 IS-IS Network Optimization

Configuration Condition

Before configuring the IPV6 IS-IS adjustment and optimization, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IPV6 IS-IS Interface Priority

The IS-IS chooses a node on the broadcast link as the DIS node. The DIS node sends the CSNP packet periodically to synchronize the link status database on the entire network. The Level-1 and Level-2 select the DIS node respectively. The interface with the highest priority is selected as the DIS node. The node with the large MAC address is selected as the DIS node for the nodes with the same priority.

Table 704 Configure the IPV6 IS-IS interface priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IS-IS interface priority	isis priority *priority-value* [level-1 | level-2]	Optional By default, the interface priority is 64.

Configure IPV6 IS-IS Passive Interface

The passive interface does not receive and transmit the IS-IS protocol packet, but still releases the directly connected network routing information of this interface. The IS-IS can reduce the bandwidth and CPU handling time through configuring the passive interface. Based on this configuration, the IS-IS can be specified to only release the directly connected network routing information of the passive interfaces and not release the directly connected network routing information of the non-passive interfaces.

Table 705Configure the IPV6 IS-IS passive interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS passive interface	passive-interface *interface-name*	Mandatory By default, the IS-IS does not have the passive interface.
Configure the IS-IS only to release the routing information of the passive interface	advertise-passive-only	Optional By default, the directly connected network routing information of the interface enabled with the IS-IS protocol is released.

Configure IPV6 IS-IS Hello Packet Parameter

1. Configure the Hello packet delivery interval.

The interface enabled with the IS-IS protocol will send the Hello packet to keep the neighboring relationship with the neighboring devices. The smaller delivery interval of the Hello packet is, the faster the network convergence is. However, more

bandwidth will be occupied.

Table 706 Configure delivery interval for the Hello packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the Hello packet delivery interval on the interface	isis hello-interval { *interval* | minimal } [level-1 | level-2]	Optional By default, the delivery interval of the Hello packet is 10s.

2. Configure the number of invalid Hello packets.

The IPV6 IS-IS calculates the neighbor relationship retention time based on the number of invalid Hello packets and informs the retention time to the neighboring device. If the neighboring device does not receive the Hello packet from this device during this period, the neighbor relationship is invalid and the routing calculation will be recalculated.

Table 707 Configure the number of invalid Hello packets

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface interface-name	-
Configure the number of invalid Hello packets on the interface	isis hello-multiplier multiplier [level-1 | level-2]	Optional By default, the number of invalid Hello packets is 3.

3. Configure to cancel the Hello packet padding function.

If MTU values on the interface at both sides of the link are inconsistent, as a result,

smaller packets can be transmitted but larger packets cannot be transmitted. To avoid such situation, the IS-IS adopts the padding Hello packet to the interface MTU value to make the neighbor relationship cannot be established. However, this method wastes the bandwidth. In actual network, there is no need to configure the padding Hello packet. Only the small Hello packets are transmitted.

Table 708 Configure to cancel the Hello packet padding function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Cancel the Hello packet padding function	no isis hello padding	Mandatory By default, the Hello packet padding function is enabled.

Configure IPV6 IS-IS LSP Packet Parameter

4. Configure the maximum survival time for the LSP packet.

Each LSP packet has a maximum survival time. When the survival time of the LSP packet reduces to 0, the LSP packet will be deleted from the link status database. The maximum survival time of the LSP packet must be larger than the LSP packet refresh interval.

Table 709 Configure the IPV6 IS-IS LSP packet parameter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration	router isis [*area-tag*]	-

Step	Command	Description
mode		
Configure the maximum survival time for the LSP packet	max-lsp-lifetime *life-time*	Optional By default, the maximum survival time of the LSP is 1200s.

5. Configure the LSP packet refresh interval.

The IS-IS protocol advertises and learns the routing through interacting each LSP packets. The nodes save the received LSP packets in the link status database. Each LSP packet has a maximum survival time and each node needs to refresh its LSP packet periodically to prevent the LSP packet maximum survival time reducing to 0 and keep the LSP packet in the entire area synchronization. Reducing the LSP packet delivery interval can accelerate the network convergence speed, but will occupy more bandwidth.

Table 710 Configure the LSP packet update packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the LSP packet refresh interval	lsp-refresh-interval *refresh-interval*	Optional By default, the packet refresh interval for the periodical packet delivery is 900s.

6. Configure the LSP packet generation interval.

Periodical refresh will generate new LSP packet. Besides, the interface status changes and network status changes will also trigger new LSP packet generation. To prevent frequently generated LSP packets occupying too much CPU resources, the user

can configure the minimum LSP packet generation interval.

Table 711 Configure the LSP packet generation interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the LSP packet generation interval	lsp-gen-interval [level-1 | level-2] *max-interval* [*initial-interval* [*secondary-interval*]]	Optional By default, the LSP packet generation interval is 50 ms.

7. Configure the LSP packet delivery interval.

Every generated LSP packet will be delivered on the interface. To avoid frequently generated LSP packet will greatly occupy the interface bandwidth. Each interface is configured with the minimum delivery interval of the LSP packet.

Table 712 Configure the LSP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the LSP packet delivery interval	isis lsp-interval *min-interval*	Optional By default, the delivery interval of the LSP packet is 33 ms.

8. Configure the LSP packet retransmission time.

On the point-to-point link, the IS-IS sends the LSP packet and the then requires the peer end to send the PSNP acknowledgement message. If the IS-IS does not receive

the acknowledgement message, the IS-IS will send the LSP packet again. The time waiting the acknowledgement message is the LSP packet retransmission interval. The retransmission interval can be set as required by the user to avoid LSP packet retransmission when the acknowledgement message is not received due to large delay.

Table 713Configure the LSP packet retransmission time

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the LSP packet retransmission time	isis retransmit-interval *interval* [level-1 | level-2]	Optional By default, the retransmission time is 5s.

9. Configure the LSP MTU value.

The IS-IS protocol packet cannot perform automatic fragmentation. In order not to affecting normal LSP packet spread, the maximum length of the LSP packet in a routing domain cannot exceed the minimum MTU value on the IS-IS interfaces of all devices. Therefore, when the interface MTU values are inconsistent on devices in the routing domain, it is recommended that the maximum length of the LSP packet is set uniformly.

Table 714 Configure the LSP MTU value

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-

Step	Command	Description
Configure the LSP packet MTU value	lsp-mtu *mtu-size* [level-1 | level-2]	Optional By default, the MTU value of the LSP packet is 1492 bytes.

Configure IPV6 IS-IS SNP Packet Parameter

1. Configure the CSNP packet delivery interval.

The selected nodes on the broadcast link need to send the CSNP packet periodically to synchronize the link status database on the entire network. The CSNP packet delivery interval is adjusted based on the actual situation.

Table 715Configure the CSNP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the CSNP packet delivery interval	isis csnp-interval *interval* [level-1 | level-2]	Optional By default, the CSNP packet delivery interval is 10s.

2. Configure the PSNP packet delivery interval

On the broadcast link, the PSNP packet synchronizes the link status database on the entire network. On the point-to-point link, the PSNP packet confirms the received LSP packet. To avoid a large number of PSNP packets being delivered over the interface. A minimum delivery interval is set for the PSNP packet and the user can change the interval dynamically. The PSNP packet delivery interval cannot be set to a too large value. If the packet delivery interval is set to a too large value, the link status

database synchronization on the entire network will be affected for the broadcast link, and the LSP packet may be redelivered caused by not timely receiving the acknowledgment message for the point-to-point link.

Table 716 Configure the PSNP packet delivery interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the PSNP packet delivery interval	isis psnp-interval *min-interval* [level-1 | level-2]	Optional By default, the PSNP packet delivery interval is 2s.

Configure IPV6 IS-IS SPF Calculation Interval

The IS-IS link status database changes will trigger the SPF routing calculation. Frequent SPF calculation will consume a mass of CPU resources and user can configure the SPF calculation interval.

Table 717 Configure the IPV6 IS-IS SPF calculation interval

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter the IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure the IS-IS SPF	spf-interval [level-1 | level-2]	Optional

Step	Command	Description
calculation interval	*maximum-interval* [*min-initial-delay* [*min-second-delay*]]	By default, *maximum-interva* l is 10s, *min-initial-delay* is 50ms, *min-second-delay* is 200ms.

Configure Maximum Number of Areas for IPV6 IS-IS

Multiple area IP addresses can be configured in an IS-IS process. Multiple area addresses are mainly applied in the following two situations that multiple Level-1 areas are combined as a Level-1 area, or a Level-1 area is divided into multiple Level-1 areas.

Table 718 Configure the maximum number of areas for the IPV6 IS-IS

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the maximum number of areas for the IS-IS	max-area-addresses *max-number*	Optional By default, the maximum number of the area addresses is 3.

Note

- This configuration must be consistent in the entire IS-IS Level-1 routing domain. Otherwise, the Level-1 neighbor cannot be established normally. The Level-2 neighbor is not affected.

Configure IPV6 IS-IS Host Name Mapping

The IS-IS uniquely identifies a intermediate system using the system ID with a fixed length of 6 bytes. When viewing the system information such as the neighbor relationship and link status database, the system ID cannot enable the user to visually associate the system ID with the host name. The IS-IS supports the mapping between the system ID and the host name to enable the user to view the system information more visually and conveniently. The IS-IS host name mapping can be configured in the following two methods:

3. Configure the IS-IS static host name mapping.

The IS-IS static host name mapping is manually established by the user between the system ID and the host name for the remote device.

Table 719 Configure the IS-IS static host name mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS static hostname mapping	hostname static *system-id host-name*	Mandatory

4. Configure the IS-IS dynamic host name mapping.

The static host name mapping requires the user to configure the system ID and host name mapping of other devices on each device in the network, which has a heavy workload. The dynamic host name mapping only configures the host name for each device, and other devices in the network can learn the host name of the device when the host name advertisement function is enabled.

Table 720 Configure the IS-IS dynamic host name mapping

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure the IS-IS dynamic host name mapping	hostname dynamic { *host-name* | area-tag | recv-only | system-name }	Mandatory By default, only the host names advertised by other devices are learnt.

Configure IPV6 IS-IS Interface to Be Added to Mesh Group

When the IS-IS interface is not added to the mesh group, the LSP packet received from an interface will be sent out on all the other IS-IS interfaces. This results in great bandwidth waste in a full mesh connected network. To avoid this situation, several IS-IS interfaces can be added to a mesh group. When an interface receives the LSP packet, it only sends the LSP packet out to the interface that is not in the same mesh group with this interface.

Table 721 Configure the IS-IS interface to be added to the mesh group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IS-IS interface to be added to the mesh group	isis mesh-group { *group-number* | blocked }	Mandatory By default, the IS-IS interface is not added to the mesh group.

Note

- The **isis mesh-group blocked** command can be used to configure the interface as the obstructive interface. The obstructive interface will not send the LSP packet actively and only send the LSP packet when receives the LSP request.

6.10.2.6 Configure IPV6 IS-IS Network Authentication

Configuration Condition

Before configuring the IPV6 IS-IS network authentication, first complete the following tasks:

- Configure the IPv6 address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IPV6 IS-IS Neighboring Authentication

When the neighbor relationship authentication is enabled for the IS-IS, the authentication information will be added to the delivered Hello packet and the received Hello packet will be authenticated. If the authentication fails, the neighbor relationship will not be established. This can prevent the neighbor relationship being established with the unreliable devices.

Table 722Configure the IS-IS neighboring authentication

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

Step	Command	Description
configuration mode		
Configure the Hello packet authentication mode	isis authentication mode { md5 | text } [level-1 | level-2]	Mandatory By default, the authentication function is not enabled.
Configure the Hello packet authentication password	isis authentication key { 0 | 7 } *password* [level-1 | level-2]	Either By default, the authentication password is not configured. The authentication password can be configured using the password chain. For details about the password chain configuration, refer to the password chain configuration chapter in the configuration manual.
	isis authentication key-chain *key-chain-name* [level-1 | level-2]	

Configure IPV6 IS-IS Route Authentication

When the routing information authentication is enabled for the IS-IS, the authentication information will be added to the LSP and SNP packets and the received LSP and SNP packets will be authenticated. If the authentication fails, the packet will be dropped directly. This can prevent the unreliable routing information spreading to the IS-IS network.

Table 723 Configure the IS-IS route authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration	router isis [*area-tag*]	-

Step	Command	Description
mode		
Configure the authentication mode of the routing information packet	authentication mode { md5 | text } [level-1 | level-2]	Mandatory By default, the authentication function is not enabled.
Configure the authentication password of the routing information packet	authentication key { 0 | 7 } *password* [level-1 | level-2]	Either By default, the authentication password is not configured. The authentication password can be configured using the password chain. For details about the password chain configuration, refer to the password chain configuration chapter in the configuration manual.
	authentication key-chain *key-chain-name* [level-1 | level-2]	

6.10.2.7 Configure IPv6 IS-IS Fast Re-routing

Configuration Conditions

Before configuring IS-IS fast re-routing, first complete the following task:

- Configure the IPv6 protocol of the interface, making the neighboring node reachable at the network layer.
- Enable the IPv6 IS-IS protocol.

Configure IPv6 IS-IS Fast Re-routing

In IPv6 IS-IS network, due to link or device failure, the packet passing through the failure point will be discarded or generate a loop. The traffic interruption caused by this will continue until the protocol reconverges, which often lasts for several seconds. In order to reduce the traffic interruption time, the IS-IS fast rerouting can be

configured. By applying the route map, the backup next hop can be set for the successfully matched route. Once the main link fails, the traffic passing through the failed link will be immediately switched to the backup link, so as to realize fast switching.

Table 724 Configure IPv6 IS-IS fast re-routing

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Enter IS-IS IPv6 address family configuration mode	address-family ipv6 unicast	-
Configure IPv6 ISIS to enable the fast re-routing function	fast-reroute route-map *route-map-name*	Mandatory By default, do not enable the IPv6 IS-IS fast re-routing function.
Configure IPv6 IS-IS to enable the dynamic fast re-routing function	fast-reroute loop-free-alternate [route-map *route-map-name*]	Mandatory By default, do not enable the IPv6 IS-IS dynamic fast re-routing function.
Configure IPv6 IS-IS to enable the pic function	pic	Mandatory After enabling the pic function, enable the auto fast re-routing function. By default, do not enable the IPv6 IS-IS pic function.

Note

- The IPv6 IS-IS fast reroute function is divided into static fast reroute and dynamic fast reroute.
- The static fast rerouting function needs to associate with the route-map, and set the next hop interface and address of the backup route in the route-map.
- At present, dynamic fast reroute only supports point-to-point network, that is, the network type of all outgoing interfaces of the device needs to be point-to-point. After configuring dynamic fast reroute, the device automatically calculates and sets the backup next hop interface and address. Dynamic fast rerouting can also be associated with route-map. Only the routes matching route map are set to back up the next hop interface and address.
- The various modes of enabling rerouting are mutually exclusive;

6.10.2.8 Configure IPv6 IS-IS GR

GR (Graceful Restart) is used to keep the route information of the forwarding layer between the local device and the neighbor device unchanged during the active/standby switchover of the devices and the forwarding is not affected. After switching the device and running again, the protocol layer of the two devices synchronizes the route information and updates the forwarding layer so that the data forwarding is not interrupted during the device switchover.

There are two roles during GR:

- GR Restarter: The device performing the protocol graceful restarting
- GR Helper: The device assisting the protocol graceful restarting

The distributed device can serve as GR Restarter and GR Helper, while the centralized device can only serve as GR Helper, assisting Restarter to complete GR.

Configuration Condition

Before configuring the IPv6 IS-IS GR, first complete the following tasks:

- Configure the IPv6 address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IPV6 IS-IS protocol.

Configure IPv6 IS-IS GR Restarter

Table 725 Configure IS-IS GR Restarter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure IS-IS to enable the GR function	nsf ietf	Mandatory By default, do not enable the GR function.
Configure the times of re-transmitting the message of notifying to enter the GR process	nsf interface-expire *resend-cnt*	Optional By default, the re-transmission times is 3.
Configure the wait time of re-transmitting the message of entering the GR process	nsf interface-timer *wait-time*	Optional By default, the wait time is 10s.

Configure IPv6 IS-IS GR Helper

GR Helper helps Restarter to complete GR. By default, the device enables the

function, and the user can disable the function via the command.

Table 726 Configure IS-IS GR helper

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IS-IS configuration mode	router isis [*area-tag*]	-
Configure IS-IS GR Helper to disable the Helper capability	nsf ietf helper disable	Mandatory Configure IS-IS GR Helper to disable the Helper capability.

6.10.2.9 IPV6 IS-IS Monitoring and Maintaining

Table 727 The IPV6 IS-IS monitoring and maintaining

Command	Description
clear isis [instance -null | *area-tag*] statistics [*interface_name*]	Clear the statistics information of the IPV6 IS-IS protocol operation
clear isis [instance -null | *area-tag*] process	Restart the IPV6 IS-IS protocol process
show isis [instance -null | *area-tag*]	Display the IPV6 IS-IS process information
show isis instance { -null | *area-tag* } ipv6 bfd-sessions	Display the BFD session information of the IPV6 IS-IS process
show isis [instance -null | *area-tag*] database [*lsp_id*] [detail] [l1 / l2] [level-1 / level-2] [self] [verbose]	Display the IPV6 IS-IS link status database information
show isis interface [*interface-name*] [detail]	Display the information of the IPV6 IS-IS protocol interface operation
show isis [instance –null | *area-tag*] ipv6 reach-info	Display the IPV6 IS-IS IPv4 subnet reachable information

Command	Description
show isis [instance –null | *area-tag*] ipv6 route	Display the IPV6 IS-IS IPv4 routing information
show isis [instance –null | *area-tag*] ipv6 topology	Display the IPV6 IS-IS IPv4 topology information
show isis [instance – null | *area-tag*] is-reach-info [level-1 | level-2]	Display the IPV6 IS-IS neighboring node information
show isis [instance –null | *area-tag*] mesh-groups	Display the IPV6 IS-IS mesh group
show isis [instance –null | *area-tag*] neighbors [*interface-name*] [detail]	Display the IPV6 IS-IS neighbor information
show isis [instance –null | *area-tag*] statistics [*interface-name*]	Display the statistics information of the IPV6 IS-IS protocol operation
show isis nsf message	Display the IPv6 IS-IS GR information
show isis nsf status	Display the IPv6 IS-IS GR status
show isis router	Display the IPV6 IS-IS host name information

6.10.3 IS-IS IPv6 Typical Configuration Example

6.10.3.1 Configure IS-IS IPv6 Basic Function

Network Requirements

- Configure the IS-IS IPv6 protocol to realize the network interconnection between devices.
- Device1 is the Level-1 router and Device2 is the Level-1-2 router. Device1 and Device2 are in the same area, Area 10. Device3 is the Level-2 router in Area 20. Device2 connects the two areas.

Network Topology

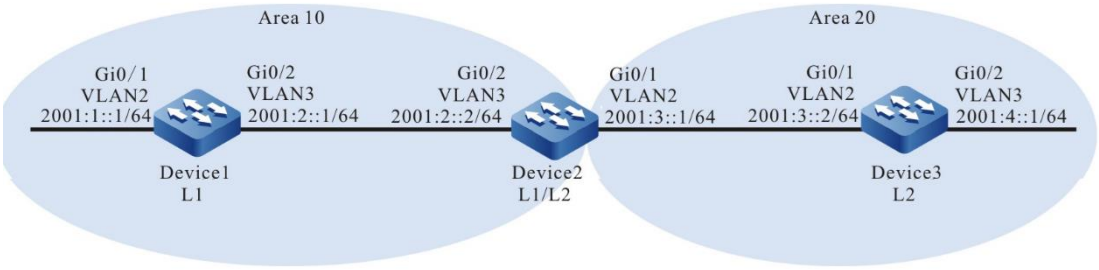


Figure 143 Networking of configuring the IPv6 IS-IS basic functions

Configuration Steps

Step 1: Configure the IPv6 address of the interfaces. (Omitted)

Step 2: Configure the IPv6 IS-IS and enable the process on the interface.

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface of Device1.

```
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)#address-family ipv6 unicast
Device1(config-isis-af)#multi-topology
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-1-2 and enable the process on the interface of Device2.

```
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)#address-family ipv6 unicast
```

```
Device2(config-isis-af)#multi-topology
Device2(config-isis-af)#exit-address-family
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 20, and type as Level-2 and enable the process on the interface of Device3.

```
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)#address-family ipv6 unicast
Device3(config-isis-af)#multi-topology
Device3(config-isis-af)#exit-address-family
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)#exit
```

Step 3: Check the result.

#View the IPv6 IS-IS neighboring 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    25 sec   L1    capable  64       0000.0000.0001.02
```

#View the IPv6 IS-IS neighboring information on Device2.

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type   System ID      Interface              State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0001  vlan2           Up    8 sec    L1    capable  64       0000.0000.0001.02
L2-LAN 0000.0000.0003  vlan3           Up    7 sec    L2    capable  64       0000.0000.0003.01
```

Device2 builds the IPv6 IS-IS neighbor with Device1 and Device3, respectively.

#View the IPv6 IS-IS neighboring 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    23 sec   L2    capable  64      0000.0000.0003.01
```

#View the routing information 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

i   ::/0 [115/10]
      via fe80::201:7aff:fe5e:6d45, 00:03:17, vlan3
L   ::1/128 [0/0]
      via ::, 16:03:18, lo0
C   2001:1::/64 [0/0]
      via ::, 00:20:11, vlan2
L   2001:1::1/128 [0/0]
      via ::, 00:20:10, lo0
C   2001:2::/64 [0/0]
      via ::, 00:19:50, vlan3
L   2001:2::1/128 [0/0]
      via ::, 00:19:49, lo0
i   2001:3::/64 [115/20]
      via fe80::201:7aff:fe5e:6d45, 00:06:48, vlan3

Device1#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L1 ::/0, flags none, metric 10, from learned, installed
      via fe80::201:7aff:fe5e:6d45, vlan3, neighbor 0000.0000.0002
L1 2001:1::/64, flags none, metric 10, from network connected
      via ::, vlan2
L1 2001:2::/64, flags none, metric 10, from network connected
      via ::, vlan3
L1 2001:3::/64, flags none, metric 20, from learned, installed
      via fe80::201:7aff:fe5e:6d45, vlan3, neighbor 0000.0000.0002
```

A default routing is in the routing table of Device1 and the next hop is Device2.

#View the routing information 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 ::, 1d:12:42:31, lo0
i   2001:1::/64 [115/20]
     via fe80::201:7aff:fe61:7a24, 00:08:32, vlan3
C   2001:2::/64 [0/0]
     via ::, 23:41:09, vlan2
L   2001:2::2/128 [0/0]
     via ::, 23:41:06, lo0
C   2001:3::/64 [0/0]
     via ::, 17:39:09, vlan3
L   2001:3::1/128 [0/0]
     via ::, 17:39:06, lo0
i   2001:4::/64 [115/20]
     via fe80::2212:1ff:fe01:101, 00:04:52, vlan2

Device2#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L1 2001:1::/64, flags none, metric 20, from learned, installed
     via fe80::201:7aff:fe61:7a24, vlan3, neighbor 0000.0000.0001
L1 2001:2::/64, flags none, metric 10, from network connected
     via ::, vlan3
L1 2001:3::/64, flags none, metric 10, from network connected
     via ::, vlan2
L2 2001:4::/64, flags none, metric 20, from learned, installed
     via fe80::2212:1ff:fe01:101, vlan2, neighbor 0000.0000.0003
```

Device2 contains the Level-1 and Level-2 routing.

#View the routing information 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 ::, 00:00:12, lo0
i   2001:1::/64 [115/30]
     via fe80::201:7aff:fe5e:6d46, 00:00:12, vlan2
i   2001:2::/64 [115/20]
     via fe80::201:7aff:fe5e:6d46, 00:00:12, vlan2
```

```
C   2001:3::/64 [0/0]
    via ::, 00:00:12, vlan2
L   2001:3::2/128 [0/0]
    via ::, 00:00:12, lo0
C   2001:4::/64 [0/0]
    via ::, 00:00:12, vlan3
L   2001:4::1/128 [0/0]
    via ::, 00:00:12, lo0

Device3#show isis ipv6 route
IS-IS Instance 100, VRF Kernel, IPv6 routes table (Counter 4):
L2 2001:1::/64, flags none, metric 30, from learned, installed
    via fe80::201:7aff:fe5e:6d46, vlan2, neighbor 0000.0000.0002
L2 2001:2::/64, flags none, metric 20, from learned, installed
    via fe80::201:7aff:fe5e:6d46, vlan2, neighbor 0000.0000.0002
L2 2001:3::/64, flags none, metric 10, from network connected
    via ::, vlan2
L2 2001:4::/64, flags none, metric 10, from network connected
    via ::, vlan3
```

Device3 learns the Level-1 route and the Level-1 leaks the route to Level-2 by default.

Note

- The metric type is the narrow metric by default. The wide metric is recommended.
- The IPv6 IS-IS entity attribute is Level-1-2 by default.

6.10.3.2 Configure IPv6 IS-IS Static Fast Re-routing

Network Requirements

- All devices are configured with the IPv6 IS-IS protocol.
- Static fast rerouting is enabled between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

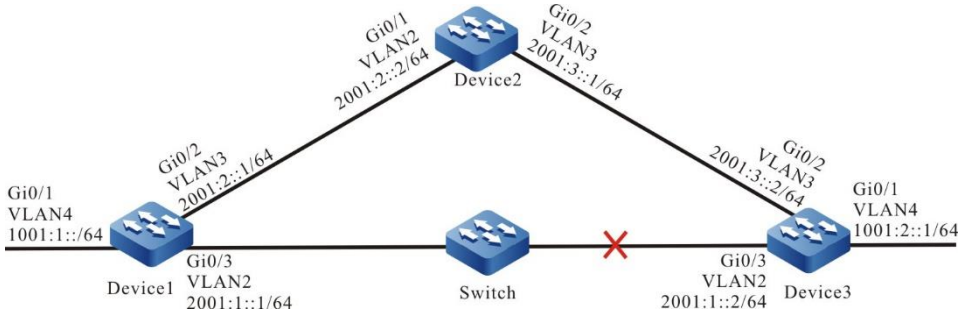


Figure 144 Networking of configuring IPv6 IS-IS static fast re-routing

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IPv6 address of the interfaces. (Omitted)

Step 2: Configure the IPv6 IS-IS and enable the process on the interface.

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-1 and enable the process on the interface of Device1.

```
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)#ipv6 router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface of Device2.

```
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)#ipv6 router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface of Device3.

```
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)#ipv6 router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)#exit
Device3(config-if-vlan4)#ipv6 router isis 100
Device3(config-if-vlan4)#exit
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next hop interface vlan3, and the next hop address 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_isis
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan2 backup-nexthop 2001:2::2
Device1(config-route-map)#exit
```

Step 4: Configure the static fast re-routing.

```
Device1(config)#router isis 100
```

```
Device1(config-isis)#address-family ipv6 unicast
Device1(config-isis-af)#fast-reroute route-map ipv6frr_isis
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit
```

Step 5: Check the result.

#View the IPv6 IS-IS route 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 ::, 06:22:27, lo0
C   1001:1::/64 [0/0]
     via ::, 06:17:34, vlan4
L   1001:1::1/128 [0/0]
     via ::, 06:17:34, vlan4
i   1001:2::/64 [115/20]
     via fe80::201:7aff:fe92:e6b6, 00:10:32, vlan2
C   2001:1::/64 [0/0]
     via ::, 01:24:08, vlan2
L   2001:1::1/128 [0/0]
     via ::, 01:24:08, vlan2
C   2001:2::/64 [0/0]
     via ::, 06:16:52, vlan3
L   2001:2::1/128 [0/0]
     via ::, 06:16:52, vlan3
i   2001:3::/64 [115/20]
     via fe80::201:7aff:fe92:e6b6, 00:29:05, vlan2
     via fe80::ced8:1fff:fe10:7aae, 00:35:19, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 FRR routing table of Device1.

```
Device1#show ipv6 frr 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
i   1001:2::/64 [115/4294967295]
     via 2001:2::2, 00:13:16, vlan3
```

You can see that the next hop of the frr route 1001:2::/64 is 2001:2::2, and the

outgoing interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6 2001:1::1 detail
Total ipv6 session number: 1
OurAddr          NeighAddr            LD/RD         State     Holddown    Interface
2001:1::1        2001:1::1            1012/1012     UP        500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:301  Remote Discriminator:301
Local State:UP  Remote State:UP  Up for: 0h:15m:38s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is established normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 06:29:08, lo0
C   1001:1::/64 [0/0]
     via ::, 06:24:15, vlan4
L   1001:1::1/128 [0/0]
     via ::, 06:24:15, vlan4
i   1001:2::/64 [115/30]
     via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
i   2001:1::/64 [115/30]
     via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
C   2001:2::/64 [0/0]
     via ::, 06:23:33, vlan3
L   2001:2::1/128 [0/0]
     via ::, 06:23:33, vlan3
i   2001:3::/64 [115/20]
     via fe80::ced8:1fff:fe10:7aae, 00:42:00, vlan3
```

6.10.3.3 Configure IPv6 IS-IS Dynamic Fast Re-routing

Network Requirements

- All devices are configured with the IPv6 IS-IS protocol.
- Dynamic fast rerouting is enabled between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

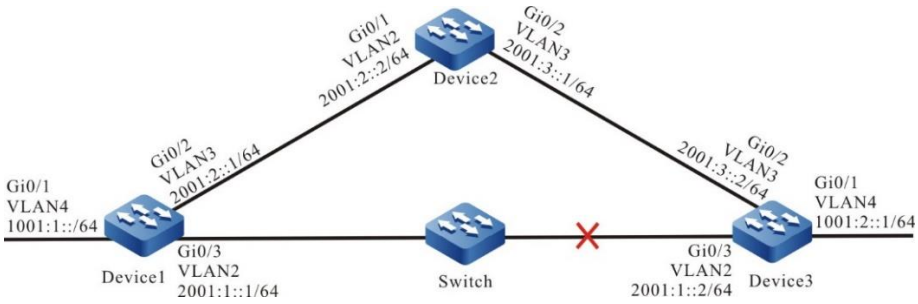


Figure 145 Networking of configuring IPv6 IS-IS dynamic fast re-routing

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IPv6 address of the interfaces. (Omitted)

Step 2: Configure the IPv6 IS-IS and enable the process on the interface.

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface of Device1. Configure the interface network type as point-to-point.

```
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)#ipv6 router isis 100
```

```
Device1(config-if-vlan2)# isis network point-to-point
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router isis 100
Device1(config-if-vlan3)# isis network point-to-point
Device1(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface of Device2. Configure the interface network type as point-to-point.

```
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)#ipv6 router isis 100
Device2(config-if-vlan2)# isis network point-to-point
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router isis 100
Device2(config-if-vlan3)# isis network point-to-point
Device2(config-if-vlan3)#exit
```

#Configure the IPv6 IS-IS process as 100, area number as 10, and type as Level-2 and enable the process on the interface of Device3. Configure the interface network type as point-to-point.

```
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)#ipv6 router isis 100
Device3(config-if-vlan2)# isis network point-to-point
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router isis 100
Device3(config-if-vlan3)# isis network point-to-point
Device3(config-if-vlan3)#exit
Device3(config-if-vlan4)#ipv6 router isis 100
```

```
Device3(config-if-vlan4)# isis network point-to-point
Device3(config-if-vlan4)#exit
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to only match 1001:2::1/64, while the other segments are filtered out.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_isis
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#exit
```

Step 4: Configure the static fast re-routing.

```
Device1(config)#router isis 100
Device1(config-isis)#address-family ipv6 unicast
Device1(config-isis-af)# fast-reroute loop-free-alternate route-map ipv6frr_isis
Device1(config-isis-af)#exit-address-family
Device1(config-isis)#exit
```

Step 5: Check the result.

#View the Ipv6 IS-IS route 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 ::, 06:22:27, lo0
C   1001:1::/64 [0/0]
     via ::, 06:17:34, vlan4
L   1001:1::1/128 [0/0]
     via ::, 06:17:34, vlan4
i   1001:2::/64 [115/20]
     via fe80::201:7aff:fe92:e6b6, 00:10:32, vlan2
C   2001:1::/64 [0/0]
     via ::, 01:24:08, vlan2
L   2001:1::1/128 [0/0]
     via ::, 01:24:08, vlan2
C   2001:2::/64 [0/0]
```

```
    via ::, 06:16:52, vlan3
L   2001:2::1/128 [0/0]
    via ::, 06:16:52, vlan3
i   2001:3::/64 [115/20]
    via fe80::201:7aff:fe92:e6b6, 00:29:05, vlan2
    via fe80::ced8:1fff:fe10:7aae, 00:35:19, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 FRR routing table of Device1.

```
Device1#show ipv6 frr 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
i   1001:2::/64 [115/4294967295]
    via fe80::ced8:1fff:fe10:7aae, 00:07:18, vlan3
```

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6  2001 :1 ::1   detail
Total ipv6 session number: 1
OurAddr          NeighAddr       LD/RD          State      Holddown    Interface
2001 :1 ::1      2001 :1 ::1     1012/1012      UP         500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:301  Remote Discriminator:301
Local State:UP  Remote State:UP  Up for: 0h:15m:38s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is established normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 06:29:08, lo0
```

```
C   1001:1::/64 [0/0]
    via ::, 06:24:15, vlan4
L   1001:1::1/128 [0/0]
    via ::, 06:24:15, vlan4
i   1001:2::/64 [115/30]
    via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
i   2001:1::/64 [115/30]
    via fe80::ced8:1fff:fe10:7aae, 00:00:01, vlan3
C   2001:2::/64 [0/0]
    via ::, 06:23:33, vlan3
L   2001:2::1/128 [0/0]
    via ::, 06:23:33, vlan3
i   2001:3::/64 [115/20]
    via fe80::ced8:1fff:fe10:7aae, 00:42:00, vlan3
```

6.11 IRMP

6.11.1 Overview

The IRMP (Internal Routing Message Protocol), compatible with the Cisco EIGRP, is a dynamic routing protocol based on the distance vector. The IRMP uses the DUAL (Diffusing Update Algorithm) to calculate the route between multiple devices in parallel, ensuring no loop circuit and fast convergence. The IRMP overcomes the low convergence speed of distance vector-based routing protocol. Besides, it does not need the link status routing protocol to run the Dijkstra algorithm and the related databases do not consume huge CPU resources or memory.

The IRMP protocol applies to the medium- and small-size network and supports multiple autonomous systems. The autonomous systems can operate independently without interfering each other.

6.11.2 IRMP Function Configuration

Table 728 IRMP function list

Configuration Task	
Configure the IRMP basic function	Enable the IRMP protocol
Configure the IRMP route generation	Configure the IRMP redistribution

Configuration Task	
Configure the IRMP route control	Configure the IRMP route summary
	Configure the IRMP administrative distance
	Configure the IRMP load balancing
	Configure the IRMP route filtering
	Configure the IRMP metric offset
	Configure the IRMP route metric value
Configure the IRMP network optimization	Configure the IRMP passive interface
	Configure the IRMP stub mode
	Configure the IRMP intelligent query
	Configure the IRMP horizontal split
	Configure the IRMP timer
	Configure the IRMP static neighbor
Configure the IRMP network authentication	Configure the IRMP authentication

6.11.2.1 Configure IRMP Basic Function

In the various IRMP configuration tasks, the IRMP protocol must be enabled first to make other function feature configurations valid.

Configuration Condition

Before configuring the IRMP basic function, first complete the following tasks:

- Configure the link layer protocol to ensure the normal communication at the link layer.
- Configure the IP address of the interface to enable the neighboring nodes

to be reachable at the network layer.

Enable IRMP Protocol

Before using the IRMP protocol, first the user must perform the following configurations:

- Establish the IRMP process.
- Configure the IRMP to cover the directly connected network segment.

Table 729 Enable the IRMP protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Establish the IRMP process and enter the IRMP configuration mode	router irmp *autonomous-system-number*	Mandatory By default, the IRMP process is not enabled.
Configure the IRMP to cover the directly connected network segment	network *ip-address* [*wildcard-mask*]	Mandatory By default, no directly connected network is covered. If the wildcard mask is not carried, the classful network address is used by default.

Note

- When establishing the IRMP neighbor, the autonomous system numbers must be consistent. Otherwise, the neighbor relationship cannot be established.

6.11.2.2 Configure IRMP Route Generation

In the IRMP, the **network** command can be used to cover the directly connected network segment routing. The external routing can be introduced using the redistribution.

Configuration Condition

Before configuring the IRMP route generation, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IRMP protocol.

Configure the IRMP redistribution

Introduce the routing generated by other protocols to the IRMP through configuring the routing redistribution. The routing of other IRMP processes can also be introduced.

Table 730 Configure the IRMP redistribution

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP redistribution	redistribute *protocol* [*process-id*] [route-map *route-map-name* / metric *bandwidth delay reliability loading mtu*]	Mandatory By default, the external routing is not redistributed.
Configure the default metric value for IRMP redistributing external routing	default-metric *bandwidth delay reliability loading mtu*	Optional

Note

- When the **default-metric** command and the **redistribute** *protocol* [*process-id*] **metric** command are configured at the same time, the later command has a higher priority.

6.11.2.3 Configure IRMP Route Control

Configuration Condition

Before configuring the IRMP route control, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IRMP protocol.

Configure IRMP Route Summary

Both the IRMP aggregated route and original detailed route exist in the local route table, but only the aggregated routing is informed to the neighbor. Thus, in the large-size network, the neighboring route table scale reduces and the network bandwidth consumed by the protocol packets also reduces.

The IRMP supports the automatic summary and interface IP address summary. The metric value of the aggregated route uses the minimum metric value of all the detailed routes.

Automatic summary

In this mode, the route is aggregated as the corresponding classful network address by the non-manual configuration. The automatic route mode only aggregates the directly connected network segment route.

Table 731 Configure the IRMP automatic summary

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP automatic summary	auto-summary	Optional By default, the IRMP automatic summary function is disabled.

Interface route summary

The interface route summary needs the user to configure the combination of a pair of destination IP address and mask. This combination aggregates the routes that are covered in this network segment.

Table 732 Configure the IRMP interface route summary

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IRMP interface IP address summary	ip summary-address irmp *autonomous-system-number ip-address mask*	Mandatory

Note

- The automatic summary only aggregates the directly connected network segment routes and nay cause all neighbors under the process to reestablish.
- The interface route summary aims at all the IRMP routes delivered from the specified interface and may cause neighbors on the specified interface

to reestablish.

- The interface route summary priors to the automatic summary.
- The interface route summary is independent with each other. That is, when the interface route summary 10.1.0.0/16 and 10.0.0.0/8 are configured at the same time, the IRMP will advertise the two summary routes simultaneously.

Configure IRMP Administrative Distance

The administrative distance performs the routing policy for the routing in the same network augment from different protocols. The smaller the administrative distance is, the higher the priority of the routing is. You can change the administrative distance of the IRMP routing to affect the routing policy.

Table 733 Configure the IRMP administrative distance

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP administrative distance	distance { irmp *internal-routes-distance external-routes-distance* | summary *summary-routes-distance* }	Optional By default, the administrative distance for the IRMP internal route is 90 and for the external route is 170. The management distance of the summary route is 5.

Note

- When configuring the IRMP administrative distance, all neighbors under the process may be reestablished.

Configure IRMP Load Balancing

The IRMP supports the equal-cost load balancing and unequal-cost load balancing. When multiple routes with the same metric values to the destination network exist, equal-cost load balancing forms. When multiple routes with the different metric values to the destination network exist, you can run the **variance** command to change the conversion factor and form the unequal-cost load balancing.

Variance defines a conversion factor, which is used to determine the scope of the unequal-cost load balancing routing. When the metric value of a non-optimal routing is smaller than the metric value of the optimal routing multiplying the variance value, this routing is selected as the unequal-cost load balancing routing.

The **maximum-paths** command is used to control the maximum number of routings for IRMP load balancing, supporting a maximum of 32 paths for load balancing. When *path-number* is set to 1, the load function is cancelled. The number of paths for IRMP load balancing includes the number of equal-cost load balancing paths and unequal-cost load balancing paths. The path selected for IRMP load balancing depends on conversion factor variance.

Table 734 Configure the IRMP load balancing

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRM conversion	variance *number*	Optional

Step	Command	Description
factor to form the unequal load balancing		By default, the conversion factor is 1.
Configure the maximum number of paths for IRMP load balancing	maximum-paths *path-number*	Optional By default, the maximum number of paths for IRMP load balancing is 4.

Configure IRMP Route Filtering

Control the received or delivered routing through configuring the ACL or prefix list. The inbound and outbound routing filtering can be configured on the interface at the same time.

Table 735 Configure the IRMP route filtering

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP route filtering	distribute-list { *access-list-name* | gateway *prefix-list-name1* | prefix *prefix-list-name2* [gateway *prefix-list-name3*] } { in | out } [*interface-name*]	Mandatory

Note

- The IRMP routing filtering only supports the standard ACL.
- You can configure the filtering on all interfaces or use the *interface-name* parameter to specify the interface for configuring filtering. When the

preceding two modes are configured at the same time, the configuration is valid when the preceding two filtering rules are set to permit.

Configure IRMP Metric Offset

By default, the IRMP routing adopts the metric value advertised by the neighbor. In some application scenarios, the metric value requires modification. The user can rectify the metric value of a specified routing by configuring the IRMP metric offset.

If the inbound metric offset is configured, the routing metric value is modified, saved in the route table, and then advertised to the neighbor upon receiving the IRMP routing. If the outbound metric offset is configured, only the metric value advertised to the neighboring routing will be modified and the local metric value remains unchanged.

Table 736 Configure the IRMP metric offset

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP metric offset	offset-list *access-list-name* { in | out } *offset-value* [*interface-name*]	Mandatory

Note

- The IRMP metric offset only supports the standard ACL.
- When configuring the IRMP metric offset, all neighbors under the process may be reestablished.

Configure IRMP Route Metric Value

The IRMP calculates a composite metric value as the rout metric value based on the link features, such as link bandwidth, delay, load, and reliability. The calculation formula is as follows:

Route metric = 256 x ([k1 x (10^7/Bandwidth) + k2 x (10^7/Bandwidth)/(256 – Load) + k3 x (Delay/10)] x [k5/(Reliability + k4)])

Where, bandwidth is in the unit of kbit/s and delay is in the unit of microsecond. Each k value indicates the weighted value of the corresponding link feature. By default, the RMP uses the link bandwidth and delay as the metric value.

Table 737 Configure the IRMP route metric value

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP route metric value	metric weights *tos k1 k2 k3 k4 k5*	Mandatory *Tos* indicates the service type, supporting only the type-0 services. By default, *k1*=*k3*=1 and *k2*=*k4*=*k5*=0. The K value must be consistent when establishing the neighbor relationship.

6.11.2.4 Configure IRMP Network Optimization

Configuration Condition

Before configuring the IRMP network optimization, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IRMP protocol.

Configure IRMP Passive Interface

The dynamic routing protocol adopts the passive interface to effectively reduce the network bandwidth consumed by the routing protocol. In the IRMP protocol, the passive interface is configured, which can suppress the IRMP packet receiving and transmitting on the specified interface. For example, if the vlan2 is configured as the passive interface, the IRMP does not receive and transmit the packet on this interface even if the **network** command is used to cover the network segment that the interface locates at.

Table 738 Configure the IRMP passive interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP passive interface	passive interface *interface-name*	Mandatory

Configure IRMP Stub Mode

Configuring the IRMP stub mode can effectively improve the IRMP network stability and reduce the resource occupation. The Stub function is usually used in the hub and spoke network topology. To enable the Stub function, you just need to configure Stub on the spoke router and do not need to change the configuration of the hub router. The spoke router specifies the advertised route type via the **irmp stub** command. The stub router does not send the query packet to the stub neighbor.

Table 739Configure the IRMP Stub

Step	Command	Description

Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP Stub	irmp stub { receive-only } | { connected / summary / redistributed }	Mandatory By default, do not configure the stub mode.

Note

- Modifying the stub configuration will result in the re-set up of all neighbors in the process.

Configure IRMP Intelligent Query

Configuring the IRMP intelligent query to control the sending of the query packet can effectively reduce the number of the packets interacted in the network and the resource occupation. After enabling the intelligent query function, the device does not send the query packet to the neighbor canceling the route, so as to reduce the number of the query packets and response packets in the network.

Table 740Configure the IRMP intelligent query

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP intelligent query	smart-query infinity-update	Mandatory By default, do not enable the intelligent query.

Configure IRMP Horizontal Split

The IRMP horizontal split indicates that the route learned by the IRMP from a certain interface will not be advertised out from this interface to avoid forming a loop.

Table 741 Configure the IRMP horizontal split

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IRMP horizontal split	ip split-horizon irmp *autonomous-system-number*	Optional By default, the horizontal split function is enabled.

Configure IRMP Timer

Configure the keep-alive timer for the IRMP neighbor.

The Hello packet of the is used to discover the neighbor and keep it alive by spreading the packet on the network using the periodical and unreliable multicast mode with the multicast address as 224.0.0.10. the default delivery interval for the Hello packet is determined by the network type of the delivery interface. The default delivery interval is 5s on the broadcast and point-to-point interface and is 60s on the NBMA interface.

The hold time indicates the invalid interval of the IRMP neighbor. When a device receives a Hello packet form its neighbor, this packet contains a hold time, which informs the maximum valid time of the neighbor to the device. If the Hello packet is not received from the neighbor when times out, it indicates that the neighbor is not reachable and the neighbor will be removed. By default, the hold time is three times of the hello interval.

Table 742 Configure the keep-alive timer for the IRMP neighbor

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IRMP hello interval	ip hello-interval irmp *autonomous-system hello-time*	Optional By default, the hello interval is set to 5s or 60s based on the network type.
Configure the IRMP hold time	ip hold-time irmp *autonomous-system-number hold-time*	Optional By default, the hold time is three times of the hello interval.

Configure the IRMP route timer.

The IRMP uses the DUAL (Diffusing Update Algorithm) to learn the routing. When the DUAL starts, the Active-timer is enabled. If the response of the queried packets is not received when the timer times out, the neighbors without response will be removed from the neighbor list. The route without response I set to Active and the route is considered as unreachable.

When the IRMP receives the neighbor request, if the local route is learnt from other neighbors, the IRMP will not respond immediately. Instead, enable a hold-down timer and then wait for a period. In the period, if the IRMP does not receive the request packet form the neighbor, it responds the packet to avoid forming the loop.

Table 743 Configure the IRMP route timer

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the active-timer timeout	timers active-time *minutes*	Optional By default, the active-timer timeout is 3 minutes.
Configure the hold down timeout	timers holddown-time *seconds*	Optional By default, the hold down timeout is 5s.

Note

- When configuring the route timer, all neighbors under the process may be reestablished.

Configure IRMP Static Neighbor

Configure the IRMP static neighbor, where all IRMP packets between neighbors adopt unicast interaction.

To run the IRMP dynamic routing protocol on the NBMA which does not support the broadcast network, such as X.25 and Frame, the static neighbor requires to be configured in pair. Otherwise the neighbor relationship will fail.

Table 744 Configure the IRMP static neighbor

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the IRMP configuration mode	router irmp *autonomous-system-number*	-
Configure the IRMP static neighbor	neighbor *neighbor-ip-address interface-name*	Mandatory

6.11.2.5 Configure IRMP Network Authentication

Configuration Condition

Before configuring the IRMP authentication, first complete the following tasks:

- Configure the IP address of the interface to enable the neighboring nodes to be reachable at the network layer.
- Enable the IRMP protocol.

Configure IRMP Authentication

Perform validity check and verification on the IRMP packet by configuring the IRMP authentication to improve the network security. The IRMP only supports the MD5 authentication.

Table 745 Configure the IRMP authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IRMP authentication function	ip message-digest-key irmp *autonomous-system-number key-id* md5 {0 | 7 } *password*	Mandatory

Note

- When the same Key-id and password are configured on the interfaces at the same time, the IRMP neighboring relationship can be established.

6.11.2.6 IRMP Monitoring and Maintaining

Table 746 The IRMP monitoring and maintaining

Command	Description
clear ip irmp error	Clear the statistics information of the IRMP error packet
clear ip irmp [*autonomous-system-number*] neighbors [*interface-name*]	Reset the IRMP neighbor
clear ip irmp traffic [*autonomous-system-number*]	Clear the statistics information for receiving and transmitting the IRMP packet
show ip irmp error	Display the statistics information of the IRMP error packet
show ip irmp interface [*autonomous-system-number*] | [*interface-name*]	Display the IRMP interface information
show ip irmp neighbor [*autonomous-system-number* | detail | *interface-name*]	Display the IRMP neighbor information
show ip irmp topology [*autonomous-system-number*] [active | detail | summary | *ip-address mask*]	Display the routing information in the IRMP topology table
show ip irmp traffic [*autonomous-system-number*]	Display the statistics information of receiving and transmitting the IRMP packet

6.11.3 IRMP Typical Configuration Example

6.11.3.1 Configure IRMP Basic Function

Network Requirements

- The IRMP operates between Device1 and Device2, establishing the neighbor and interacting the route.

Network Topology

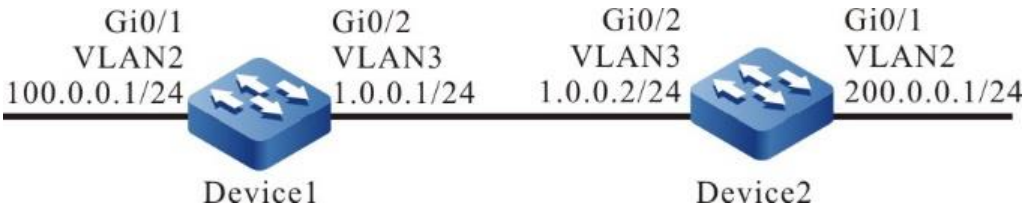


Figure 146 Networking of the IRMP basic function

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 100.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 200.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

Step 3: Check the result.

#View the IRMP neighbor information of Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address         Interface                Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
1.0.0.2         vlan3                    11       00:01:19  1         16        2
```

#View the IRMP neighbor information of Device2.

```
Device2#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address         Interface                Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
1.0.0.1         vlan3                    11       00:01:19  1         16        2
```

It can be viewed that the IRMP neighbor is established between Device1 and Device2I

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan3
P >200.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan3
P >100.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 00:27:02, vlan3
E   200.0.0.0/24 [90/30720] via 1.0.0.2, 00:15:07, vlan3
C   100.0.0.0/24 is directly connected, 00:27:14, vlan2
C   127.0.0.0/8 is directly connected, 137:46:13, lo0
```

Device1 learns the routing 200.0.0.0/24 advertised by Device2.

#View the IRMP topology table and route table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor
```

```
P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan3
P >200.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >100.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.1 (30720/28160), vlan3

Device2#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 00:20:12, vlan3
C   200.0.0.0/24 is directly connected, 00:19:53, vlan2
E   100.0.0.0/24 [90/30720] via 1.0.0.1, 00:08:41, vlan3
C   127.0.0.0/8 is directly connected, 361:04:08, lo0
```

Device2 learns the routing 100.0.0.0/24 advertised by Device1.

6.11.3.2 Configure IRMP Redistribution

Network Requirements

- The OSPF neighbor is established between Device3 and Device2 and the interface directly connected routing 200.0.0.0/24 and 210.0.0.0/24 are advertised to Device2.
- The IRMP neighbor is established between Device1 and Device2. When Device2 redistributing the OSPF routing to the IRMP, only the routing 200.0.0.0/24 instead of the routing 210.0.0.0/24 is advertised to Device1 through the routing policy control.

Network Topology

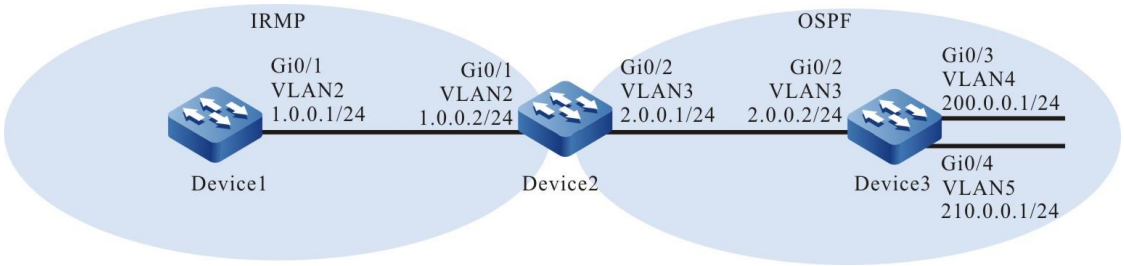


Figure 147 Networking of the IRMP route redistribution

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the OSPF.

#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 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 210.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device2.

```
Device2#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 07:39:21, vlan2
C   2.0.0.0/24 is directly connected, 00:03:36, vlan3
C   127.0.0.0/8 is directly connected, 57:04:58, lo0
O   200.0.0.0/24 [110/2] via 2.0.0.2, 00:01:10, vlan3
O   210.0.0.0/24 [110/2] via 2.0.0.2, 00:01:10, vlan3
```

In the route table, it can be viewed that Device2 learns the OSPF routing 200.0.0.0/24 and 210.0.0.0/24 advertised by Device3.

Step 3: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#View the IRMP neighbor informatione of Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address         Interface               Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
1.0.0.2         vlan2                   11       00:01:19  1         16        2
```

The IRMP neighbor is successfully established between Device1 and Device2.

Step 4: Configure the IRMP to redistribute the OSPF routing and to coordinate with the routing policy.

#Configure the routing policy to match the ACL only permitting the routing 200.0.0.0/24 on Device2 and to coordinate with the routing policy when the IRMP redistributing the OSPF routing.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map ospf_to_irmp
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
Device2(config)#router irmp 100
Device2(config-irmp)#redistribute ospf 100 route-map ospf_to_irmp
Device2(config-irmp)#exit
```

Note

- When configuring the routing policy, both the prefix list and ACL can establish the matching rule. The difference lies in that the prefix list can accurately match the route mask, but the ACL cannot match the route mask.

Step 5: Check the result.

#View the IRMP topology table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P  200.0.0.0/24, 1 successors, FD is 28160
       via RedisOSPF 100 (28160/0)
```

It can be viewed that Device2 successfully distributes the OSPF routing to the IRMP.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor
P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >200.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external
C   1.0.0.0/24 is directly connected, 07:47:01, vlan2
C   127.0.0.0/8 is directly connected, 07:55:23, lo0
Ex  200.0.0.0/24 [170/30720] via 1.0.0.2, 00:00:06, vlan2
```

It can be viewed that Device1 learns the routing 200.0.0.0/24.

Caution

- In the actual application, if there are two or more edge routers in the autonomous system, you are advised to not redistribute routes between different routing protocols. If necessary, configure the routing control policies such as filtering and summary on the edge router in the

autonomous system to prevent generating routing loop.

6.11.3.3 Configure IRMP Metric Offset

Network Requirements

- The IRMP protocol operates among Device1, Device2, Device3, and Device4 for interconnection.
- Device1 learns the routing 200.0.0.0/24 from Device2 and Device3 at the same time.
- Configure the routing metric offset at the receiving direction on Device1to enable Device1 to choose the routing advertised by Device2 preferentially.

Network Topology

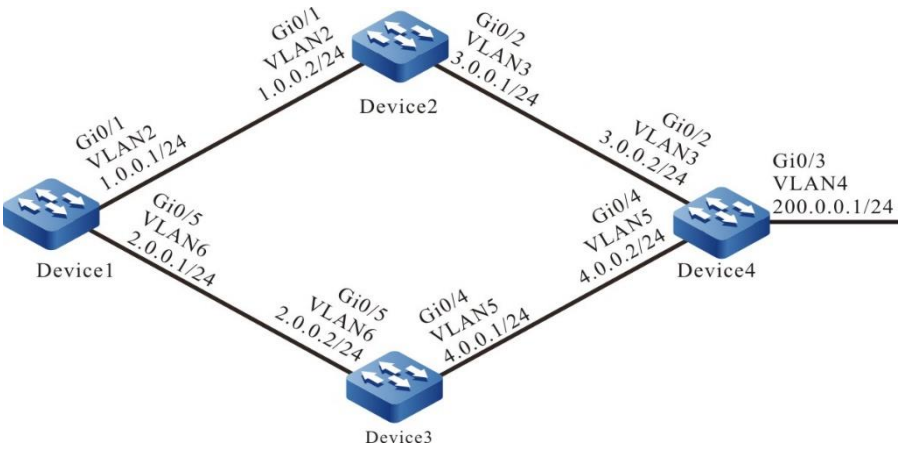


Figure 148 Networking of the IRMP metric offset

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
```

```
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 2.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 4.0.0.0 0.0.0.255
Device3(config-irmp)#exit
```

Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 4.0.0.0 0.0.0.255
Device4(config-irmp)#network 200.0.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#View the IRMP neighbor information of Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address         Interface              Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
1.0.0.2         vlan2                  11       00:10:37  10        0         2
2.0.0.2         vlan6                  12       00:10:15  9         0         2
```

#View the IRMP neighbor information of Device4.

```
Device4#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address         Interface              Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
3.0.0.1         vlan3                  14       00:11:37  13        0         2
4.0.0.1         vlan5                  12       00:10:45  12        0         2
```

Device1 sets up the IRMP neighbor with Device2, Device3 respectively. Device4 sets up the IRMP neighbor with Device2, Device3 respectively.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan6
P >3.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 30720
      *via 2.0.0.2 (30720/512), vlan6
P >200.0.0.0/24, 2 successors, FD is 33280
      *via 2.0.0.2 (33280/30720), vlan6
      *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 13:16:35, vlan2
C   2.0.0.0/24 is directly connected, 13:19:24, vlan6
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:03:22, vlan2
E   4.0.0.0/24 [90/30720] via 2.0.0.2, 00:22:01, vlan6
C   127.0.0.0/8 is directly connected, 22:27:25, lo0
E   200.0.0.0/24 [90/33280] via 2.0.0.2, 00:21:22, vlan6
            [90/33280] via 1.0.0.2, 00:03:22, vlan2
```

There are two load balancing routing to the network segment 200.0.0.0/24 in Device1 route table. The forwarding paths to the network segment are Device1→Device2→Device4 and Device1→Device3→Device4.

Step 3: Configure the IRMP metric offset.

#Configure the offset list on Device1. Add metric value 100 to the interface connected to Device3 by the specified routing to enable the total metric value going through Device3 is larger than that going through Device2.

```
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
```

```
Device1(config)#router irmp 100
Device1(config-irmp)#offset-list 1 in 100 vlan6
Device1(config-irmp)#exit
```

Step 4: Check the result.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan6
P >3.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 30720
      *via 2.0.0.2 (30720/512), vlan6
P >200.0.0.0/24, 2 successors, FD is 33280
      *via 1.0.0.2 (33280/30720), vlan2
       via 2.0.0.2 (33380/30820), vlan6

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 13:33:22, vlan2
C   2.0.0.0/24 is directly connected, 13:36:11, vlan6
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:06:56, vlan2
E   4.0.0.0/24 [90/30720] via 2.0.0.2, 00:05:43, vlan6
C   127.0.0.0/8 is directly connected, 22:44:12, lo0
E   200.0.0.0/24 [90/33280] via 1.0.0.2, 00:06:56, vlan2
```

After the metric offset is configured, Device1 chooses the routing 200.0.0.0/24 advertised by Device2.


Note

- Configuring the IRMP offset list may cause the neighbor to be reestablished.

6.11.3.4 Configure IRMP Route Filtering

Network Requirements

- The IRMP operated between Device1 and Device2 for routing interaction.
- Device1 learns two routing 2.0.0.0/24 and 3.0.0.0/24 advertised by Device2 and Device1 only reserves the routing information of 2.0.0.0/24.

Network Topology

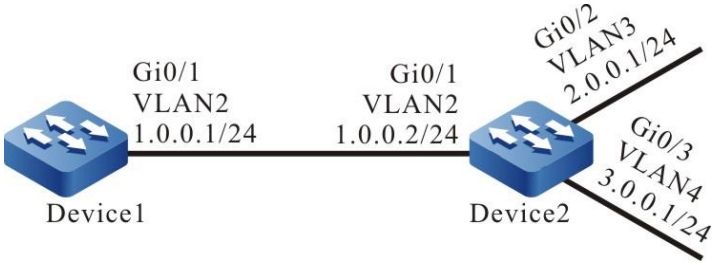


Figure 149 Networking of the IRMP route filtering

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
```

```
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 2.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#View the IRMP neighbor inofrmation of Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 1
Address         Interface              Hold(s)  Uptime    SeqNum   Srtt(ms)  Rto(s)
1.0.0.2         vlan2          11       00:05:00  3        0        2
```

It can be viewed that the IRMP neighbor is successfully established between Device1 and Device2.

#View the route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 00:11:29, vlan2
E   2.0.0.0/24 [90/30720] via 1.0.0.2, 00:07:43, vlan2
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:07:40, vlan2
C   127.0.0.0/8 is directly connected, 00:19:50, lo0
```

Device1 learns the routing 2.0.0.0/24 and 3.0.0.0/24.

Step 3: Configure the route filtering.

#Configure the ACL rule to only permit the routing 2.0.0.0/24 on Device1 and configure the inbound filtering list to coordinate with the ACL in the IRMP.

```
Device1(config)#ip access-list standard 1
```

```
Device1(config-std-nacl)#permit 2.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#router irmp 100
Device1(config-irmp)#distribute-list 1 in
Device1(config-irmp)#exit
```

Note

- When configuring the route filtering, the prefix list and ACL can establish the matching rule. The difference lies in that the prefix list can accurately match the route mask, but the ACL cannot match the route mask.

Step 4: Check the result.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 00:22:33, vlan2
E   2.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:18, vlan2
C   127.0.0.0/8 is directly connected, 00:30:55, lo0
```

Device1 only learns the routing 2.0.0.0/24, but the routing 3.0.0.0/24 is successfully filtered.

Note

- Configuring the **distribute-list** command may cause the IRMP neighbor to be reestablished.

6.11.3.5 Configure IRMP Route Summary

Network Requirements

- The IRMP protocol operates among Device1, Device2, Device3, and Device4 for routing interaction,
- Device1 learns two routing 100.1.0.0/24 and 100.2.0.0/24 from Device. To reduce the route table scale of Device1, it is required that Device2 only releases the route summary 100.0.0.0/14 to Device1.

Network Topology

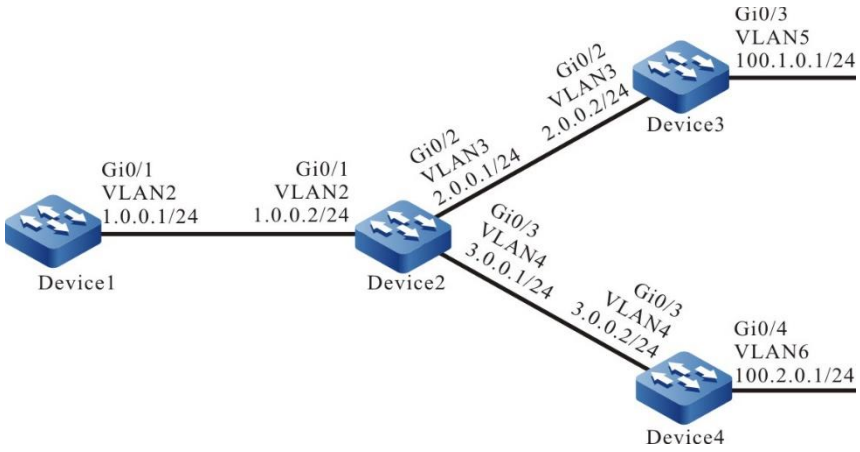


Figure 150 Networking of the IRMP route summary

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 2.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 100.1.0.0 0.0.0.255
Device3(config-irmp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 100.2.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#View the IRMP neighbor inofrmation of Device2.

```
Device2#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 3
Address         Interface              Hold(s)  Uptime    SeqNum   Srtt(ms)  Rto(s)
1.0.0.1         vlan2                  11       00:05:04  4        0         2
2.0.0.2         vlan3                  14       00:04:42  3        16        2
3.0.0.2         vlan4                  11       00:04:00  2        0         2
```

Device2 successfully establishes the IRMP neighbor with Device1, Device3, and Device4, respectively.

#View the topology table and route table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
```

```
        *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
        *via Connected (28160/0), vlan3
P >3.0.0.0/24, 1 successors, FD is 28160
        *via Connected (28160/0), vlan4
P >100.1.0.0/24, 1 successors, FD is 30720
        *via 2.0.0.2 (30720/28160), vlan3
P >100.2.0.0/24, 1 successors, FD is 30720
        *via 3.0.0.2 (30720/28160), vlan4

Device2#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 08:12:36, vlan2
C   2.0.0.0/24 is directly connected, 00:36:51, vlan3
C   3.0.0.0/24 is directly connected, 00:12:06, vlan4
E   100.1.0.0/24 [90/30720] via 2.0.0.2, 00:10:03, vlan3
E   100.2.0.0/24 [90/30720] via 3.0.0.2, 00:00:08, vlan4
C   127.0.0.0/8 is directly connected, 57:38:13, lo0
```

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
        > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
        *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
        *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
        *via 1.0.0.2 (30720/28160), vlan2
P >100.1.0.0/24, 1 successors, FD is 33280
        *via 1.0.0.2 (33280/30720), vlan2
P >100.2.0.0/24, 1 successors, FD is 33280
        *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 08:09:15, vlan2
```

```
E   2.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:19, vlan2
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:17, vlan2
E   100.1.0.0/24 [90/33280] via 1.0.0.2, 00:12:53, vlan2
E   100.2.0.0/24 [90/33280] via 1.0.0.2, 00:02:57, vlan2
C   127.0.0.0/8 is directly connected, 08:17:36, lo0
```

Both Device1 and Device2 learn routing 100.1.0.0/24 and 100.2.0.0/24.

Step 3: Configure the IRMP route summary.

#Configure Device2 and configure the IRMP route summary 100.0.0.0/14 on the interface connected to Device1.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ip summary-address irmp 100 100.0.0.0 255.252.0.0
Device2(config-if-vlan2)#exit
```

Step 4: Check the result.

#View the IRMP topology table of Device2.

```
Device2#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan3
P >3.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan4
P  100.0.0.0/14, 1 successors, FD is 30720
       via AddrSumm (30720/0)
P >100.1.0.0/24, 1 successors, FD is 30720
      *via 2.0.0.2 (30720/28160), vlan3
P >100.2.0.0/24, 1 successors, FD is 30720
      *via 3.0.0.2 (30720/28160), vlan4
```

A route summary 100.0.0.0/14 is generated on Device2.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
```

```
        > - FIB route, * - FIB successor
P >1.0.0.0/24, 1 successors, FD is 28160
        *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 30720
        *via 1.0.0.2 (30720/28160), vlan2
P >3.0.0.0/24, 1 successors, FD is 30720
        *via 1.0.0.2 (30720/28160), vlan2
P >100.0.0.0/14, 1 successors, FD is 33280
        *via 1.0.0.2 (33280/30720), vlan2
Device1#show ip 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, E - IRMP, EX - IRMP external
C   1.0.0.0/24 is directly connected, 08:18:49, vlan2
E   2.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:54, vlan2
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:04:54, vlan2
E   100.0.0.0/14 [90/33280] via 1.0.0.2, 00:04:54, vlan2
C   127.0.0.0/8 is directly connected, 08:27:10, lo0
```

It can be viewed that only the route summary100.0.0.0/14 instead of the corresponding detailed route100.1.0.0/24 and 100.2.0.0/24 exists on Device1.

Note

- Configuring the IRMP route summary in the interface mode may cause the neighbor to be reestablished.

6.11.3.6 Configure IRMP Load Balancing

Network Requirements

- The IRMP protocol operates among Device1, Device2, Device3, and Device4 for routing interaction.
- Device1 learns the routing 200.0.0.0/24 from Device2 and Device3 at the same time. Modify the bandwidth of interface vlan4 on Device1 to enable Device1 to preferentially choose the routing 200.0.0.0/24 learned from Device2.

- Device1 is required to transfer data to the network segment200.0.0.0/24 simultaneously on lines Device1→Device2→Device4 and Device1→Device3→Device4.

Network Topology

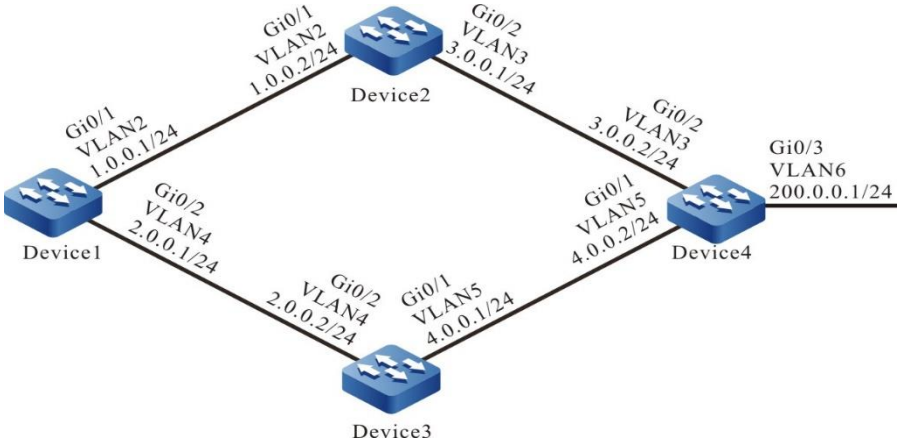


Figure 151 Networking of the IRMP unequal-cost load balancing

Configuration Steps

Step 1: Configure the IP address of the interfaces. (Omitted)

Step 2: Configure the IRMP.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router irmp 100
Device1(config-irmp)#network 1.0.0.0 0.0.0.255
Device1(config-irmp)#network 2.0.0.0 0.0.0.255
Device1(config-irmp)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router irmp 100
Device2(config-irmp)#network 1.0.0.0 0.0.0.255
Device2(config-irmp)#network 3.0.0.0 0.0.0.255
Device2(config-irmp)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router irmp 100
```

```
Device3(config-irmp)#network 2.0.0.0 0.0.0.255
Device3(config-irmp)#network 4.0.0.0 0.0.0.255
Device3(config-irmp)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router irmp 100
Device4(config-irmp)#network 3.0.0.0 0.0.0.255
Device4(config-irmp)#network 4.0.0.0 0.0.0.255
Device4(config-irmp)#network 200.0.0.0 0.0.0.255
Device4(config-irmp)#exit
```

#View the IRMP neighbor information of Device1.

```
Device1#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address         Interface               Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
1.0.0.2         vlan2                   11       00:10:37  10        0         2
2.0.0.2         vlan4                   12       00:10:15  9         0         2
```

#View the IRMP neighbor information of Device4.

```
Device4#show ip irmp neighbor
IP-IRMP neighbors for process 100 Total neighbor 2
Address         Interface               Hold(s)  Uptime    SeqNum    Srtt(ms)  Rto(s)
3.0.0.1         vlan3                   14       00:11:37  13        0         2
4.0.0.1         vlan5                   12       00:10:45  12        0         2
```

Device1 sets up the IRMP neighbor with Device2, Device3 respectively. Device4 sets up the IRMP neighbor with Device2, Device3 respectively.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
      > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
      *via Connected (28160/0), vlan4
P >3.0.0.0/24, 1 successors, FD is 30720
      *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 30720
      *via 2.0.0.2 (30720/512), vlan4
P >200.0.0.0/24, 2 successors, FD is 33280
      *via 2.0.0.2 (33280/30720), vlan4
```

```
        *via 1.0.0.2 (33280/30720), vlan2

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 13:16:35, vlan2
C   2.0.0.0/24 is directly connected, 13:19:24, vlan4
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:03:22, vlan2
E   4.0.0.0/24 [90/30720] via 2.0.0.2, 00:22:01, vlan4
C   127.0.0.0/8 is directly connected, 22:27:25, lo0
E   200.0.0.0/24 [90/33280] via 2.0.0.2, 00:21:22, vlan4
                 [90/33280] via 1.0.0.2, 00:03:22, vlan2
```

There are two load balancing routing to the network segment 200.0.0.0/24 in Device1 route table. The forwarding paths to the network segment are Device1→Device2→Device4 and Device1→Device3→Device4.

Step 3: Change the interface bandwidth.

#Change the bandwidth of the interface connected to Device1 and Device3 to 10000Kbps.

```
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#bandwidth 10000
Device1(config-if-vlan4)#exit
```

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
        > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
        *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 258560
        *via Connected (258560/0), vlan4
P >3.0.0.0/24, 1 successors, FD is 30720
        *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 261120
        *via 2.0.0.2 (261120/28160), vlan4
P >200.0.0.0/24, 2 successors, FD is 33280
        *via 1.0.0.2 (33280/30720), vlan2
```

```
        via 2.0.0.2 (263680/30720), vlan4

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 28:44:11, vlan2
C   2.0.0.0/24 is directly connected, 00:14:05, vlan4
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:10:11, vlan2
E   4.0.0.0/24 [90/284160] via 2.0.0.2, 00:07:57, vlan4
C   127.0.0.0/8 is directly connected, 220:26:51, lo0
E   200.0.0.0/24 [90/33280] via 1.0.0.2, 00:10:11, vlan2
```

After modifying the interface bandwidth, Device1 preferentially chooses the routing 200.0.0.0/24 advertised by Device2.

Step 4: Configure the IRMP unequal-cost load balancing.

#Configure Device1 and configure the load balancing conversion factor as 100.

```
Device1(config)#router irmp 100
Device1(config-irmp)#variance 100
Device1(config-irmp)#exit
```

For details about the load balancing conversion factor, refer to the load balancing chapter in the IRMP function configuration.

Step 5: Check the result.

#View the topology table and route table of Device1.

```
Device1#show ip irmp topology
IP-IRMP Topology Table for process 100
Codes:  P - Passive, A - Active, H - Holddown, D - Hidden
       > - FIB route, * - FIB successor

P >1.0.0.0/24, 1 successors, FD is 28160
       *via Connected (28160/0), vlan2
P >2.0.0.0/24, 1 successors, FD is 28160
       *via Connected (28160/0), vlan4
P >3.0.0.0/24, 1 successors, FD is 30720
       *via 1.0.0.2 (30720/28160), vlan2
P >4.0.0.0/24, 1 successors, FD is 284160
       *via 2.0.0.2 (284160/28160), vlan4
```

```
P >200.0.0.0/24, 2 successors, FD is 33280
      *via 1.0.0.2 (33280/30720), vlan2
      *via 2.0.0.2 (263680/30720), vlan4

Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.0.0.0/24 is directly connected, 28:47:15, vlan2
C   2.0.0.0/24 is directly connected, 00:17:08, vlan4
E   3.0.0.0/24 [90/30720] via 1.0.0.2, 00:13:15, vlan2
E   4.0.0.0/24 [90/284160] via 2.0.0.2, 00:11:00, vlan4
C   127.0.0.0/8 is directly connected, 220:29:54, lo0
E   200.0.0.0/24 [90/33280] via 1.0.0.2, 00:13:15, vlan2
              [90/263680] via 2.0.0.2, 00:00:12, vlan4
```

Routing 200.0.0.0/24 on Device1 forms the unequal-cost load balancing. Data will be transmitted for load balancing on these two paths based on the inverse ratio of the metric value.

6.12 BGP

6.12.1 Overview

Border Gateway Protocol (BGP) is a routing protocol that exchanges Network Layer Reachability Information (NLRI) between Autonomous Systems (ASs). Internal Gateway Protocols (IGPs) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS), focus mainly on finding accurate paths, taking network nodes (such as routers, layer-3 switches, multi-NIC hosts) as the routing units. Different from IGPs, External Gateway Protocols (EGPs) focuses mainly on controlling the routing direction, taking AS networks as the routing units.

BGP is used for interconnection between AS networks. It supports routing information exchange between ASs. It is usually used for large-scale network aggregation and network core. Its application layer determines that BGI has the

following features when compared with IGP:

- BGP uses the TCP protocol to transmit packets through service port 179. TCP ensures the reliability of transmission, so BGP need not provide an independent transmission control policy for reliable transmission of information.
- BGP updates routes in incremental mode, that is, it informs its neighbors of route changes only when route properties are changed, or a route is added or deleted. This mode greatly decreases network bandwidth that is occupied by BGP in transmitting routes.
- BGP is an AS-based distance vector protocol. It carries AS path properties in routing packets to solve the routing loop problem.
- BGP routes have abundant properties. You can modify the properties by applying a routing policy. In this way, you can control route filtering and selection freely.
- BGP has two neighbor types, Interior Border Gateway Protocol (IBGP) and External Border Gateway Protocol (EBGP). Between different types of neighbors, different route advertisements and routing policies are used.

6.12.2 BGP Function Configuration

Table 747 BGP function list

Configuration Tasks	
Configure a BGP neighbor.	Configure an IBGP neighbor.
	Configure an EBGP neighbor.
	Configure a BGP passive neighbor.
	Configure an MP-BGP neighbor.
	Configure MD5 authentication for BGP

Configuration Tasks	
	neighbors.
Configure BGP route generation.	Configure BGP to advertise local routes.
	Configuring BGP to redistribute routes.
	Configure BGP to advertise the default route.
Configure BGP route control.	Configure BGP to advertise aggregated routes.
	Configure the administrative distance of BGP routes.
	Configure routing policies in the outgoing direction of a BGP neighbor.
	Configure a routing policies in the incoming direction of a BGP neighbor.
	Configure the maximum number of routes that a BGP neighbor receives.
	Configure the maximum number of BGP load balancing routes.
Configure BGP route properties.	Configure the BGP route weight.
	Configure the MED property of a BGP route.
	Configure the Local-Preference property of a BGP route.
	Configure the AS_PATH property of a BGP route.
	Configure the NEXT-HOP property of a BGP route.
	Configure the community property of a BGP

Configuration Tasks	
	route.
Configure BGP network optimization.	Configure the keep-alive time of BGP neighbors.
	Configure BGP route detection time.
	Configure quick disconnection of EBGP neighbors.
	Configure the BGP route suppression function.
	Configure the BGP neighbor refresh capability.
	Configure the BGP neighbor soft reset capability.
	Configure the ORF capability of BGP neighbors.
Configure a large-scale BGP network.	Configure a BGP peer group.
	Configure a BGP route reflector.
	Configure a BGP confederation.
Configure BGP GR	Configure BGP GR Helper
Configure BGP to coordinate with BFD.	Configure EBGP to coordinate with BFD.
	Configure IBGP to coordinate with BFD.

6.12.2.1 Configure BGP Neighbor

Configuration Condition

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 addresses of the interfaces have been configured so that the adjacent network nodes are reachable at the network layer.

Configure an IBGP Neighbor

1. Perform basic configuration.

In configuring an IBGP neighbor, you need to set the AS of the neighbor to be the same as the AS of the local device. You can configure a Router ID for a device. The Router ID is used to uniquely identify a BGP device in setting up a BGP session. If no Router ID is configured for a device, the device selects a Router ID from interface addresses. The rules for selection are as follows:

- Select the biggest IP address from loopback interface IP addresses as the Router ID.
- If no loopback interface is configured with an IP address, select the biggest IP address from the IP addresses of other interfaces as the Router ID.
- Only when an interface is in the UP status can the IP address of the interface be elected as the Router ID.

Table 748 Configure an IBGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	Mandatory. By default, BGP is disabled.
Configure a Router ID for the BGP device.	bgp router-id *router-id*	Optional. By default, the device selects a Router ID from interface addresses. The loopback interface and large

Step	Command	Description
		IP address have the priorities.
Configure an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no IBGP neighbor is created.
Activate the capability of an IBGP neighbor in transmitting and receiving IPv4 unicast routes.	neighbor { *neighbor-address* | *peer-group-name* } activate	Optional. By default, the IBGP neighbor's capability in transmitting and receiving IPv4 unicast routes is activated automatically.
Configure a description for an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } description *description-string*	Optional. By default, no description is configured for an IBGP neighbor.

2. Configure the source address of a TCP session.

BGP uses the TCP protocol to transmit packets through service port 179. TCP features reliable transmission, ensuring that BGP protocol packets can be properly transmitted to its neighbors.

Table 749 Configure the source address of a TCP session

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	-

Step	Command	Description
Configure an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no IBGP neighbor is created.
Configure the source address of a TCP session of an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } update-source { *interface-name* | *ip-address* }	Mandatory. By default, the TCP session automatically selects the address of a routing output interface as the source address.

Note

- If there exist load balancing routes, the source addresses must be configured for TCP sessions of BGP neighbors. If TCP session source addresses are not configured, if the neighbors have different optimal routes, they may use different output interfaces as their source addresses. In this way, BGP sessions may fail to set up within a period of time.

Configure an EBGP Neighbor

1. Perform basic configuration.

In configuring an EBGP neighbor, you need to set the AS of the neighbor to be different from the AS of the local device.

Table 750 Configure an EBGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure an EBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no EBGP neighbor is created.

2. Configure a non-direct-connect EBGP neighbor

EBGP neighbors are located in different operation networks, and they are usually connected by a direct-connect physical link. Therefore, the default TTL value for the IP packets between EBGP neighbors is 1. In non-direct-connect operation networks, you can use a command to set the TTL value of IP packets so as to set up a BGP connection.

Table 751 Configure a non-direct-connect EBGP neighbor

Step	Command	Description
Enter the 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*	Mandatory. By default, no EBGP neighbor is created.
Configure the source address of a TCP session of an EBGP	neighbor { *neighbor-address* | *peer-group-name* } update-source	Optional.

Step	Command	Description
neighbor.	{ *interface-name* | *ip-address* }	By default, the TCP session automatically selects the address of a routing output interface as the source address.
Allow non-direct-connect EBGP neighbors to set up a connection.	neighbor { *neighbor-address* | *peer-group-name* } ebgp-multihop [*ttl-value*]	Mandatory. By default, non-direct-connect devices are not allowed to form EBGP neighbors.

Configure a BGP Passive Neighbor

In some special application environments, the BGP passive neighbor function is in need. After the passive neighbor function is enabled, the BGP does not initiate the TCP connection request for setting up a BGP neighbor relation; instead, it waits for the neighbor's connection request before setting up a neighbor relation. By default, neighbors initiate connection requests to each other. If connections conflict, they select an optimal TCP connection to form a BGP session. Before configuring a BGP passive neighbor, you need to configure a BGP neighbor.

Table 752 Configure a BGP passive neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure a BGP neighbor.	neighbor { *neighbor-address* |	Mandatory.

Step	Command	Description
	peer-group-name } remote-as *as-number*	By default, no BGP neighbor is created.
Configure a BGP passive neighbor.	neighbor { *neighbor-address* | *peer-group-name* } passive	Mandatory. By default, no passive neighbor is activated.

Configure an MP-BGP Neighbor

By default, BGP neighbors are activated in the IPv4 unicast address family, and they have the capability of transmitting and receiving IPv4 unicast routes. Neighbors need to be activated by using a command in other address families, such as multicast address family, VRF address family, and LS unicast address family so that they have the capability of transmitting and receiving the required routes. Before configuring an MP-BGP neighbor, you need to configure a BGP neighbor.

Table 753 Configure an MP-BGP neighbor

Step	Command	Description
Enter the 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*	Mandatory. By default, no BGP neighbor is created.
Enter the BGP IPv4 configuration mode.	address-family ipv4 multicast	Mandatory. By default, after entering the BGP configuration mode,

Step	Command	Description
		the user is in unicast address family mode.
Activate neighbors in BGP IPv4 multicast address family.	neighbor { *neighbor-address* | *peer-group-name* } activate	Mandatory. By default, global neighbors are deactivated in multicast address family mode.
Exit the BGP IPv4 configuration mode.	exit-address-family	-
Enter the BGP IPv4 VRF configuration mode.	address-family ipv4 vrf *vrf-name*	-
Configure neighbors in BGP IPv4 VRF address family mode.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no BGP neighbor is created.
Activate neighbors in IPv4 VRF address family mode.	neighbor { *neighbor-address* | *peer-group-name* } activate	Optional. By default, neighbors are activated in BGP IPv4 VRF configuration mode.
Exit the BGP IPv4 VRF configuration mode.	exit-address-family	-
Enter the BGP LS config mode.	address-family link-state unicast	-
Activate neighbors in BGP LS unicast address family mode.	neighbor { *neighbor-address* | *peer-group-name* } activate	Mandatory. By default, global neighbors are deactivated in VPN address family mode.
Exit the BGP LS configuration mode.	exit-address-family	-

Note

- The neighbors that are configured in BGP configuration mode and BGP IPv4 unicast configuration mode are global neighbors, and the neighbors that are configured in BGP IPv4 VRF configuration mode belong only to the VRF address family.

Configure MD5 Authentication for BGP Neighbors

BGP supports configuring MD5 authentication to protect information exchange between neighbors. MD5 authentication is implemented by the TCP protocol. Two neighbors must be configured with the same authentication password before a TCP connection can be set up; otherwise, if the TCP protocol fails in MD5 authentication, the TCP connection cannot be set up. Before configuring MD5 authentication for BGP neighbors, you need to configure BGP neighbors.

Table 754 Configure MD5 authentication for BGP neighbors

Step	Command	Description
Enter the 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	Mandatory. By default, no BGP neighbor is created.
Configure the MD5 authentication for BGP neighbors.	neighbor { neighbor-address | peer-group-name } password [0 | 7] password-string	Mandatory. By default, no MD5 authentication is started for

Step	Command	Description
		BGP neighbors.

6.12.2.2 Configure BGP Route Generation

Configuration Condition

Before configuring BGP route generation, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure BGP to Advertise Local Routes

BGP can use the **network** command to introduce the routes of the IP route table into the BGP route table. Only when there are routes that match completely the **network** prefix and mask can the routes be introduced into the BGP route table and advertised.

In advertising a local route, you can apply a route map for the route, and you can also specify the route as the backdoor route. The backdoor route takes EBGP routes as local BGP routes and uses the administrative distance of local routes. This allows IGP routes to have higher priorities than EBGP routes. At the same time, backdoor routes will not be advertised to EBGP neighbors.

Table 755 Configure BGP to advertise local routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to advertise local routes.	network *ip-address mask* [route-map *rtmap-name* [backdoor] |	Mandatory. By default, BGP does not

	backdoor]	advertise local routes.

Note

- The Origin property type of the local routes that are advertised by BGP is IGP.
- If you run the **network backdoor** command for an EBGP route, the administrative distance of the EBGP route changes to the local route administrative distance. (By default, the EBGP route administrative distance is 20, and the local route administrative distance is 200.) Then, the administrative distance of the EBGP route is smaller than the administrative distance of the default IGP route. In this way, the IGP route is selected with priority, forming a backdoor link between EBGP neighbors.
- The route map applied to the local routes that are advertised by BGP supports match options, including as-path, community, extcommunity, ip address, ip nexthop, and metric, and it supports the set options, including as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

Configure BGP to Redistribute Routes

BGP is not responsible for route learning. It focuses mainly on managing route properties so as to control the route direction. Therefore, BGP redistributes IGP routes to generate BGP routes and advertise the BGP routes to neighbors. When BGP redistributes IGP routes, it can apply a routing diagram.

Table 756 Configure BGP to redistribute routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to redistribute IGP routes.	redistribute { connected | irmp *as-number* | isis [*area-tag*] [match *isis-level*] | ospf *as-number* [match *route-sub-type*] | rip | static } [route-map *map-name* / metric *value*]	Mandatory. By default, BGP does not redistribute IGP routes.

Note

- The Origin property type of the IGP routes that are advertised by BGP is INCOMPLETE.
- The route map applied to other protocol routes that are redistributed by BGP supports match options, including as-path, community, extcommunity, ip address, ip nexthop, and metric, and it supports the set options, including as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

Configure BGP to Advertise the Default Route

Before BGP advertises a default route to neighbors, the default route needs to be introduced. Two ways of introducing the default routes are available: Running the **neighbor default-originate** command to generate a BGP default route, and running the **default-information originate** command to redistribute the default route of

another protocol.

The default route that is generated by running the **neighbor default-originate** command is route 0.0.0.0/0 that is automatically generated by BGP. The default route that is redistributed by running the **default-information originate** command is route 0.0.0.0/0 of the redistributed protocol introduced by BGP.

Table 757 Configure BGP to advertise the default route

Step	Command	Description
Enter the 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*]	Mandatory. By default, BGP does not generate the default route.
Configure the default route of another protocol redistributed by BGP.	default-information originate	Mandatory. By default, BGP does not redistribute the default route of another protocol.

Note

- In configuring BGP to redistribute the default route of another protocol, you need to configure BGP to redistribute routes.
- In configuring BGP to generate a default route, you can apply a route map to the route.
- The route map that is applied to the default route that is generated by BGP

supports set options, including as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weigh.

6.12.2.3 Configure BGP Route Control

Configuration Condition

Before configuring BGP route control, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure BGP to Advertise Aggregated Routes

In a large-scale BGP network, to decrease the number of routes that are advertised to neighbors or effectively control BGP routing, you can configure a BGP aggregated route.

Table 758 Configure BGP to advertise aggregated routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to advertise aggregated routes.	aggregate-address *ip-address mask* [as-set / summary-only / route-map *rtmap-name*]	Mandatory. By default, BGP does not aggregate routes.

Note

- When configuring BGP to advertise aggregated routes, you can specify the

summary-only option so that BGP advertises only aggregated routes. This decreases the number of routes that are advertised.

- You can specify the **as-set** option to generate aggregation routes with the AS_PATH property.
- You can also apply a route map to the aggregation routes so as to set more abundant properties for the aggregation routes.

Configure the Administrative Distance of BGP Routes

In the IP route table, each protocol controls the administrative distance of routing. The smaller the administrative distance is, the higher the priority is .BGP affects routing by specifying the administrative distances of specified network segments. The administrative distances of the routes that cover the specified network segments will be modified. Meanwhile, ACL is applied to filter the network segments that are covered by the routes, that is, only the administrative distances of the network segment that are allowed by the ACL can be modified.

The **distance bgp** command is used to modify the management distances of external, internal, and local BGP routes. The **distance** command is only used to modify the administrative distances of specified network segments. The **distance** command has a higher priority than the **distance bgp** command. The network segments that are covered by the **distance** command use the administrative distance that is specified by the command, while the network segments that are not covered by the distance command use the administrative distance that is specified by the **distance bgp** command.

Table 759 Configure the administrative distance of a BGP route

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
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 routes is 20, the administrative distance of IBGP routes is 200, and the administrative distance of local routes is 200.
Configure the administrative distance of a specified network segment.	distance *administrative-distance ip-address mask* [*acl-name*]	

Configure Routing Policies in the Outgoing Direction of a BGP Neighbor

BGP route advertisement or routing is implemented based on the powerful routing properties. When advertising routes to neighbors, you can apply routing policies to modify route properties or filter some routes. Currently, the routing policies that can be applied in the outgoing direction include:

- distribute-list: Distribution list.
- filter-list: AS_PATH property filtration list.
- prefix-list: IP prefix list.
- route-map: Route map.

Table 760 Configure routing policies in the outgoing direction of a BGP neighbor

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

Step	Command	Description
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Apply the distribution list in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } distribute-list *access-list-name* out	You can select multiple options. (However, the distribution list and the IP prefix list cannot be configured at the same time.) By default, no routing policy is configured in the outgoing direction of a BGP neighbor.
Apply the AS_PATH property filtration list in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } filter-list *aspath-list-name* out	
Apply the IP prefix list in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* out	
Apply a route map in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* out	

Note

- After configuring the routing policy in the outgoing direction of a BGP neighbor, you need to reset the neighbor to validate the settings.
- If you apply a route map in the outgoing direction of a route reflector, this changes only the NEXT-HOP property.
- For how to configure a filtration list, refer to the "Configure AS-PATH" section of the "Routing Policy Tools" chapter.
- In configuring routing policies in the outgoing direction of a BGP neighbor, you can configure multiple policies at the same time. BGP applies routing policies in the sequence of **distribute-list**, **filter-list**,

prefix-list, and **route-map**. If a former policy is rejected, the latter policies will not be applied. The routing information can be advertised only after it passes all the configured policies.

- The route map that is applied in the outgoing direction of a BGP route supports match options, including as-path, community, extcommunity, ip address, ip nexthop, and metric, and it supports the set options, including as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

Configure Routing Policies in the Incoming Direction of a BGP Neighbor

BGP can apply routing policies to filter received routing information or modify route properties. Similar to the policies applied in the outgoing directions, four polices are applied in the incoming directions:

distribute-list: Distribution list.

filter-list: AS_PATH property filtration list.

prefix-list: IP prefix list.

route-map: Route map.

Table 761 Configure Routing Policies in the Incoming Direction of a BGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Apply the distribution list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } distribute-list *access-list-name* in	You can select multiple options. (However, the distribution list and the IP

Apply the AS_PATH property filtration list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } filter-list *aspath-list-name* in	prefix list cannot be configured at the same time.) By default, no policy is applied in the incoming direction.
Apply the IP prefix list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* in	
Apply a route map in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in	

Note

- After configuring the routing policy in the incoming direction of a BGP neighbor, you need to reset the neighbor to validate the settings.
- In configuring routing policies in the incoming direction of a BGP neighbor, you can configure multiple policies at the same time. BGP applies routing policies in the sequence of **distribute-list**, **filter-list**, **prefix-list**, and **route-map**. If a former policy is rejected, the latter policies will not be applied. A route can be added into the database after it passes all the configured policies.
- The routing policies applied in the incoming direction of a BGP route support match options, including as-path, community, extcommunity, ip address, ip nexthop, and metric, and they support the set options, including as-path, comm-list, community, extcommunity, ip next-hop, local-preference, metric, origin, and weight.

Configure the Maximum Number of Routes that a BGP Receives from a Neighbor

You can limit the number of routes that a BGP device receives from a specified neighbor. Once the number of routes the BGP receives from the neighbor reaches a

threshold, an alarm is generated or the neighbor is disconnected.

Table 762 Configure the maximum number of routes that a BGP Receives from a neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the maximum number of routes that a BGP receives from a neighbor.	neighbor { *neighbor-address* | *peer-group-name* } maximum-prefix *prefix-num* [*threshold-value*] [warning-only]	Mandatory. By default, the number of routes that a BGP receives from a neighbor is not limited.

Note

- If the warning-only option is not specified, after the number of routes that the BGP receives from the neighbor reaches the maximum number, the BGP session is automatically disconnected.
- If the warning-only option is specified, after the number of routes that the BGP receives from the neighbor reaches the maximum number, a warning message is displayed, but route learning continues.

Configure the Maximum Number of BGP Load Balancing Routes

In a BGP networking environment, if several paths with the same cost are available to reach the same destination, you can configure the number of BGP load balancing routes for load balancing.

Table 763 Configure the Maximum number of BGP load balancing routes

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the maximum number of IBGP load balancing routes.	maximum-paths ibgp *number*	Mandatory. By default, IBGP does not support load balancing routes.
Configure the maximum number of EBGP load balancing routes.	maximum-paths *number*	Mandatory. By default, EBGP does not support load balancing routes.

Note

- After the maximum number of EBGP load balancing routes is configured, load balancing takes effect only when EBGP routes are selected with priority.
- In different BGP configuration modes, the commands for configuring the maximum number of load balancing routes are different. For details, refer to the description of **maximum-paths** in the BGP technical manual.

6.12.2.4 Configure BGP Route Properties

Configuration Condition

Before configuring BGP route properties, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure the BGP Route Weight

In BGP routing, the first rule is to compare the weights of routes. The larger the weight of a route is, the higher the priority it has. The weight of a route is the local property of the device, and it cannot be transferred to other BGP neighbors. The value range of a route weight is 1-65535. By default, the weight of a route that has been learnt from a neighbor is 0, and the weights of all routes that are generated by the local device are all 32768.

Table 764 Configure the BGP route weight

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the weight of a route of a neighbor or peer group.	neighbor { *neighbor-address* | *peer-group-name* } weight *weight-num*	Mandatory. By default, the weight of a route of a neighbor is 0.

Configure the MED Property of a BGP Route

Multi-Exit Discriminator (MED) properties are used to select the optimal route for the traffic that enters an AS. If the other routing conditions are the same and BGP learns several routes with the same destination from different EBGP neighbors, BGP select the route with the minimum MED value as the optimal ingress.

MED sometimes is also called external metric. It is marked as a "metric" in the BGP route table. BGP advertises the MED properties of the routes that it has learnt

from neighbors to IBGP neighbors, but BGP does not advertise the MED properties to EBGP neighbors. Therefore, MED properties are applicable to only adjacent ASs.

1. Configure BGP to allow comparing MEDs of neighbor routes from different ASs.

By default, BGP implements MED route selection only among the routes that are from the same AS. However, you can run the **bgp always-compare-med** command to let BGP ignore the limitation on the same AS in MED route selection.

Table 765 Configure BGP to allow comparing MEDs of neighbor routes from different ASs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to allow comparing MEDs of neighbor routes from different ASs.	bgp always-compare-med	Mandatory. By default, BGP allows only to compare MEDs of neighbor routes from the same AS.

2. Configure BGP to sort and select MEDs according to AS_PATH groups.

By default, BGP is not enabled to sort and select MEDs according to route AS_PATH groups. To enable the function, run the **bgp deterministic-med** command. In route selection, all routes are organized based on AS_PATHs. In each AS_PATH group, routes are sorted based MED values. The route with the minimum MED value is selected as the optimal route in the group.

Table 766 Configure BGP to sort and select MEDs according to AS_PATH groups

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
BGP sorts and selects MEDs according to AS_PATH groups	bgp deterministic-med	Mandatory By default, do not enable BGP to sort and select MEDs according to AS_PATH groups.

3. Configure to compare MEDs of routes in the local confederation.

By default, the MED values of EBGP routes from different ASs are not compared. The setting is valid for the EBGP routes of confederations. To enable comparison of MED values of routes of the local confederation, run the **bgp bestpath med confed** command.

Table 767 Configure BGP to compare MEDs of routes in the local confederation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to compare MED values of routes in the local confederation.	bgp bestpath med confed	Mandatory. By default, the MED values of routes in the local confederations will not be compared.

4. Configure a route map to modify MED properties.

In transmitting and receiving routes, you can apply a route map to modify MED properties.

Table 768 Configure a route map to modify MED properties

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configuring a route map to modify MED properties.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an MED property, you can use the **set metric** command to modify the MED property. For details, refer to Routing Policy Tools-Technical Manual-set metric.
- After the **neighbor attribute-unchanged** command is configured, the MED properties of neighbors cannot be changed by the route map that is applied.

Configure the Local-Preference Property of a BGP Route

Local-Preference properties are transferred only between IBGP neighbors. Local-Preference is used to select the optimal egress of an AS. The route with the maximum Local-Preference will be selected with priority.

The value range of Local-Preference is 0-4294967295. The larger the value is, the higher priority the route has. By default, the Local-Preference value of all the routes

that are advertised to IBGP neighbors is 100. You can use the **bgp default local-preference** command or the route map to modify the Local-Preference property value.

1. Configure BGP to modify the default Local-Preference property.

Table 769 Configure BGP to modify the default local-preference property

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the default value of BGP Local-Preference property.	bgp default local-preference *local-value*	Optional. By default, the Local-Preference value is 100.

2. Configure the route map to modify the Local-Preference property.

Table 770 Configure the route map to modify the local-preference property

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the route map to modify the Local-Preference property.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, the route map is not applied to any neighbor.

Note

- In configuring a route map to modify the Local-Preference property, you can use the **set local-preference** command to modify the Local-Preference property. For details, refer to Routing Policy Tools-Technical Manual-**set local-preference**.

Configure the AS_PATH Property of a BGP Route

1. Configure BGP to ignore AS_PATHs in route selection.

If the other conditions are the same, BGP selects the route with the shortest AS-PATH in route selection. To cancel route selection based on AS_PATHs, run the **bgp bestpath as-path ignore** command.

Table 771 Configure BGP to ignore AS_PATHs in route selection

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to ignore AS_PATHs in route selection.	bgp bestpath as-path ignore	Mandatory. By default, the AS_PATH values are compared in route selection.

2. Configure the number of local ASs that BGP allows to repeat.

To prevent routing loops, BGP checks the AS_PATH properties of the routes that are received from neighbors, and the routes containing the local AS number will be discarded. However, you can run the **neighbor allowas-in** command to allow the AS_PATH properties of the routes that the BGP receives to contain the local AS

number, and you can configure the number of ASs that can be contained.

Table 772 Configure the number of local ASs that BGP allows to repeat

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the number of ASs that are allowed to repeat.	neighbor { *neighbor-address* | *peer-group-name* } allowas-in [*as-num*]	Mandatory. By default, the AS_PATH properties of the routes that are received from neighbors do not allow the local AS number.

3. Configure BGP to remove the private AS number when advertising routes to neighbors.

In a large-scale BGP network, the AS_PATH properties of routes contain federation or community property. By default, BGP provides the private AS properties when it advertises routes to neighbors. To mask private network information, run the **neighbor remove-private-AS** command to remove the private AS number.

Table 773 Configure BGP to Remove the Private AS number when advertising routes to neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to remove the	neighbor { *neighbor-address* |	Mandatory.

Step	Command	Description
private AS number when advertising routes to neighbors.	*peer-group-name* } remove-private-AS	By default, when BGP advertise routes to neighbors, it provides the private AS number.

4. Configure to check the validity of the first AS number of an EBGP route.

When BGP advertises a route to EBGP neighbors, it compresses the local AS number to the starting position of the AS_PATH, and the AS that advertises the route first is located at the end. Usually, the first AS of a route that EBGP receives must be the same as the neighbor AS number; otherwise, the route will be discarded.

Table 774 Configure to check the validity of the first AS number of an EBGP route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure to check the validity of the first AS number of an EBGP route.	bgp enforce-first-as	Mandatory. By default, BGP does not enable the mechanism for checking the first AS number.

5. Configure a route map to modify AS_PATH properties.

BGP supports configuring a route map to modify AS_PATH properties. You can run the **set as-path prepend** command to add more routing properties so as to affect neighbor routing. In using the **set as-path prepend** function, first use the local AS to add AS_PATH. If you use another AS, the AS must be emphasized to prevent the AS from rejecting routes that are advertised to it.

Table 775 Configure a Route map to modify AS_PATH properties

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure a route map to modify AS_PATH properties.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an AS_PATH property, you can use the **set as-path prepend** command to modify the AS_PATH property. For details, refer to Routing Policy Tools-Technical Manual-**set as-path**.

Configure the NEXT-HOP Property of a BGP Route

When BGP advertises routes to IBGP neighbors, it does not change the routing properties (including the NEXT-HOP property). When BGP advertises the routes that are learned from EBGP neighbors to IBGP neighbors, you can run the **neighbor next-hop-self-**command to modify the next-hop property of the routes advertised to BGP neighbors to the local IP address. You can apply a route map to modify the next hop property.

1. Configure BGP to use the local IP address as the next hop of a route.

Table 776 Configure BGP to use the local IP address as the next hop of a route

Step	Command	Description
Enter the 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 routes.	neighbor { *neighbor-address* | *peer-group-name* } next-hop-self	Mandatory. By default, the next-hop property of the routes that are advertised to EBGP neighbors is set to the local IP address, and the next-hop property of the routes that are advertised to IBGP neighbors keeps unchanged.

Note

- When BGP is configured to use the local IP address as the next hop of a route, if you run the **neighbor update-source** command to configure the source address of a TCP session, the source address is used as the next hop address; otherwise, the IP address of the output interface of the advertising device is selected as the local IP address.

2. Configure a route map to modify NEXT-HOP properties.

BGP supports configuring a route map to modify NEXT-HOP properties. You can run the **set ip next-hop** command to modify the next hop property.

Table 777 Configure a route map to modify NEXT-HOP properties

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure a route map to modify NEXT-HOP properties.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an NEXT-HOP property, you can use the **set ip next-hop** command to modify the NEXT-HOP property. For details, refer to Routing Policy Tools-Technical Manual-**set ip next-hop**.

Configure the Community Property of a BGP Route

When BGP advertises routes to neighbors, it can be configured to send the community property. You can apply a route map to a specified neighbor in the incoming and outgoing directions to match the community properties.

Community property is used to identify a group of routes so as to apply a routing policy to the group of routes. Two types of community property are available: standard and extended. The standard community property consist of 4 bytes, providing the properties such as NO_EXPORT, LOCAL_AS, NO_ADVERTISE, and INTERNET. The extended property consist of eight bytes, providing Route Target (RT) and Route Origin (RO) properties.

1. Configure BGP to advertise route community property to neighbors.

The **neighbor send-community** enables you to advertise standard community

property or extended community property or both types of property to neighbors.

Table 778 Configure BGP to advertise route community property to neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to advertise route community property to neighbors.	neighbor { *neighbor-address* | *peer-group-name* } send-community [both | extended | standard]	Mandatory. By default, the community property is not advertised to any neighbor.

Note

- After neighbors are activated in VPNv4 address family, standard and extended community properties are automatically advertised to neighbors.

2. Configure a route map to modify the community property.

BGP supports configuring a route map to modify the route community property. You can use the **set communtiy** to command to modify the community property.

Table 779 Configure a route map to modify the community property

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure a route map to modify the BGP route	neighbor { *neighbor-address* | *peer-group-name* } route-map	Mandatory. By default, no route map is

community property	*rtmap-name* in | out	applied to any neighbor.

Note

- In configuring a route map to modify community property, you can use the **set community** command to modify the community property. For details, refer to Routing Policy Tools-Technical Manual-**set community**.

6.12.2.5 Configure BGP Network Optimization

Configuration Condition

Before configuring BGP network optimization, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure the Keep-alive Time of BGP Neighbors

After a BGP session is successfully set up, keep-alive messages are sent periodically between the neighbors to maintain the BGP session. If no keep-alive message or Update packet is received from the neighbor within the hold time, the BGP session will be disconnected owing to timeout. The keep-alive time is equal to or smaller than 1/3 of the hold time.

Table 780 Configure the keep-alive time of BGP neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration	router bgp *autonomous-system*	-

mode.		
Configure global BGP keep-alive time and hold time.	timers bgp *keepalive-interval holdtime-interval*	Optional. By default, the keepalive timer is 60s, the hold timer is 180s, and the session re-connection timer is 120s.
Configure the keepalive time and hold time 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 hold time that are set for a specified neighbor have higher priorities than the global BGP keepalive time and hold time.
- Neighbors negotiate and then take the minimum hold time as the hold of the BGP session between the neighbors.
- If the keepalive time and hold time are both set to 0, the neighbor keepalive/hold function is canceled.
- If the keepalive time is longer than 1/3 of the hold time, the BGP session sends keepalive packets at the interval of 1/3 the hold time.

Configure BGP Route Detection Time

BGP mainly aims at implementing a routing process, with ASs as the routing units. Within an AS, IGP is used for routing. Therefore, BGP routes often rely on IGP routes. If the next hops or output interfaces of IGP routes that BGP relies on change, BGP detects IGP routes periodically to update BGP routes. BGP also update local BGP routes during the detection interval.

Table 781 Configure BGP route detection time

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP route detection time.	bgp scan-time *time*	Optional. By default, the BGP route detection time is 60s.

Caution

- If the BGP route detection time is set too small, BGP detect routes frequently, affecting the device performance.

Configure Quick Disconnection of EBGP Neighbors

After a BGP session is successfully set up, Keepalive messages are sent periodically between the neighbors to maintain the BGP session. If no Keepalive message or Update packet is received from the neighbor within the hold time, the BGP session will be disconnected owing to timeout. You can configure direct-connect EBGP neighbors to disconnect a BGP connection immediately after a connecting interface is down, without waiting for BGP keepalive timeout. If the EBGP neighbor quick disconnection function is cancelled, the EBGP session does not respond to an interface down event; instead, the BGP session is disconnected after timeout.

Table 782 Configure quick disconnection of EBGP neighbors

Step	Command	Description

Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure quick disconnection of EBGP neighbors.	bgp fast-external-failover	Optional. By default, EBGP's quick processing capability in responding to the direct-connect interface down event is enabled.

Configure the BGP Route Suppression Function

Flapping routes in a network may cause instability of the network. You can configure route attenuation to damp this type of routes so as to decrease the effect of flapping routes on the network.

A frequently flapping route will be allocated with a penalty. If the penalty exceeds the suppression threshold, the route will not be advertised to neighbors. The penalty should not be kept beyond the maximum suppression time. If no flapping occurs on the route within the half-life period, the penalty will be halved. If the penalty is lower than the threshold value, the route can be advertised to neighbors again.

- Half-life period: It is the time in which the penalty of a route is halved.
- Reuse threshold: It is the threshold for the route to resume normal use.
- Suppression threshold: It is the threshold for route suppression.
- Maximum suppression time: It is the maximum time that a route is suppressed

Table 783 Configure the BGP route suppression function

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the BGP route attenuation period.	bgp dampening [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | route-map *rtmap-name*]	Mandatory. By default, the route suppression function is disabled. After the function is enabled, the default route suppression half-life period is 15 minutes, the route reuse time is 750, the route suppression threshold is 2000, the maximum route suppression time is 60 minutes, and the route penalty unreachable half-life period is 15 minutes.

Caution

- Route flapping not only contains addition and deletion of routes, but also contains route property changes such as next hop and MED property changes.

Configure the BGP Neighbor Refresh Capability

If the routing policy or route selection policy that is applied to a BGP neighbor changes, the route table needs to be refreshed. One way of refreshing the route table is to reset the BGP connection so as to reset the BGP session. However, this mode may result in BGP route flapping, affecting normal services. The other way is more graceful, that is, configuring the local BGP device to support the route refresh capability. If a neighbor needs to reset a route, it advertises the Route-Refresh message to the local

device. After receiving the Route-Refresh message, it sends the route to the neighbor again. In this way, the route table is dynamically refreshed without the need of disconnecting the BGP session.

Table 784 Configure the BGP Neighbor refresh capability

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enable the BGP neighbor refresh capability.	neighbor { *neighbor-address* | *peer-group-name* } capability route-refresh	Optional. By default, the BGP neighbor refresh capability is enabled.

Configure the BGP Neighbor Soft Reset Capability

If the routing policy or route selection policy that is applied to a BGP neighbor changes, the route table needs to be refreshed. One way of refreshing the route table is to reset the BGP connection so as to reset the BGP session. However, this mode may result in BGP route flapping, affecting normal services. Another way is more graceful, that is, configuring the local BGP device to support the route refresh capability. There is still another way, that is, enabling the soft reset capability of the local BGP device. By default, the BGP device reserves the routing information of each neighbor. After enabling its neighbor soft reset capability, it refreshes the neighbor routes that are kept on the local device. At this time, BGP sessions are not disconnected.

Table 785 Configure the BGP neighbor soft reset capability

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enable the BGP neighbor soft reset capability.	neighbor { *neighbor-address* | *peer-group-name* } soft-reconfiguration inbound	Mandatory. By default, the neighbor soft reset function is disabled.

Configure the ORF Capability of BGP Neighbors

BGP implements accurate route control through abundant routing properties. It usually applies routing policies in the incoming and outgoing directions. This mode is a local BGP behavior. BGP also supports the Outbound Route Filtering (ORF) capability. It advertises the local ingress policy to its neighbors through Route-refresh packets, and then the neighbors apply the policy when they advertise routes to the local BGP device. This greatly decreases the number of exchanged route refresh packets between BGP neighbors.

To achieve successful negotiation of the ORF capability, ensure that:

- The ORF capability is enabled for both neighbors.
- "ORF send" and "ORF receive" must match. That is, if one end is "ORF send", the other end must be "ORF both" or "ORF receive". If one end is "ORF receive", the other end must be "ORF send" or "ORF both".
- The "ORF send" end must be configured with a prefix list in the incoming direction.

Table 786 Configure the ORF capability of BGP neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Apply a prefix list in the incoming direction of a neighbor.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* in	Mandatory. By default, no prefix list is applied to any BGP neighbor.
Configure a neighbor to support the ORF capability.	neighbor { *neighbor-address* | *peer-group-name* } capability orf prefix-list { both | receive | send }	Mandatory. By default, a neighbor does not support the ORF capability.

6. 12. 2. 6 Configure Large-Scale BGP Network

Configuration Condition

Before configuring a large-scale BGP network, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure a BGP Peer Group

A BGP peer group is a group of BGP neighbors that are configured with the same configuration policy. Any configuration that is performed on a BGP peer group will take effect on all members of the peer group. In this way, by configuring the peer group, you can perform centralized management and maintenance on the neighbors.

Table 787 Configure a BGP peer group

Step	Command	Description
Enter the 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	Mandatory. By default, no peer group is configured, and a neighbor is not in any peer group.
Add a neighbor into the peer group.	neighbor *neighbor-address* peer-group *peer-group-name*	

Note

- The configuration on a peer group takes effect on all members of the peer group.
- After a neighbor is added into a peer group, if some configurations of the neighbor are the same as the configurations of the peer group, the configurations of the neighbor are deleted.
- If routing policies are configured in the incoming and outgoing directions of a peer group, after the routing policies are changed, the changes do not take effect on the neighbors that have been added into the peer group. To apply the changed routing policies on the peer group members, you need to reset the peer group.

Configure a BGP Route Reflector

In a large-scale BGP network, it is required that IBGP neighbors are fully connected, that is, each BGP needs to set up connections with all IBGP neighbors. In

this way, in a network which contains N BGP neighbors, the number of BGP connections is N*(N-1)/2. The larger the number of connections is, the larger the number of route advertisements is. Configuring a BGP Route Reflector (RR) is a method of reducing the number of network connections. Multiple IBGPs are categorized into a group. In this group, a BGP is specified to act as the RR, while other BGPs act as client, and BGPs that are not in the group act as non-clients. Clients set up peer relations only with the RR while they do not set up peer relations with other BGPs. This reduces the number of mandatory IBGP connections, and the number of connections is N-1.

The following shoes the routing principles of the BGP RR:

- The RR reflects the routes that it learns from non-client IBGP neighbors only to clients.
- The RR reflects the routes that it learns from clients to all clients and non-clients except the clients that initiate the routes.
- The RR reflects the routes that it learns from EBGP neighbors to all clients and non-clients.

Table 788 Configure a BGP route reflector

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure an RR cluster ID.	bgp cluster-id { *cluster-id-in-ip* | *cluster-id-in-num* }	Mandatory. By default, the route ID is used as the RR cluster ID.
Configure a neighbor as a client of the RR.	neighbor { *neighbor-address* | *peer-group-name* } route-	Mandatory. By default, no client is

Step	Command	Description
	reflector-client	specified as a client of the RR.
Configure the route reflection function between BGP neighbors.	bgp client-to-client reflection	Optional. By default, the route reflection function is enabled between RR clients.

Note

- An RR cluster ID is used to identify an RR area. An RR area can contain multiple RRs, and the RRs in the RR area have the same RR cluster ID.

Configure a BGP Confederation

In a large-scale BGP network, it is required that IBGP neighbors are fully connected, that is, each BGP needs to set up connections with all IBGP neighbors. In this way, in a network which contains N BGP neighbors, the number of BGP connections is N*(N-1)/2. The larger the number of connections is, the larger the number of route advertisements is. Configuring BGP confederations is another way of reducing the number of network connections. An AS area is divided into multiple sub-AS areas, and each AS area forms a confederation. IBGP is adopted within a confederation to provide full connections, and sub-AS areas in the confederation are connected through EBGP connections. This effectively reduces the number of BGP connections.

In configuring BGP confederations, you need to assign a confederation ID for each confederation and specify members for the confederation. In the case of route reflection, only the route reflector is required to support route reflection. However, in the case of a confederation, all members in a confederation must support the confederation function.

Table 789 Configure a BGP confederation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp autonomous-system	-
Create a BGP confederation ID.	bgp confederation identifier as-number	Mandatory. By default, no AS number is configured for a confederation.
Configure members for the confederation.	bgp confederation peers as-number-list	Mandatory. By default, no sub-AS number is configured for a confederation.

Note

- A confederation ID is used to identify the sub-ASs of the confederation. Confederation members are divided into the sub-ASs.

6.12.2.7 Configure BGP GR

Graceful Restart (GR) is used in active/standby switchover between devices. During the GR, the routing information of the local device and neighbor devices keep unchanged at the forwarding layer, and data forwarding is not affected. After the switchover is completed and the new device starts to run, the two devices synchronize routing information at the protocol layer and update the forwarding layer so that data forwarding is not interrupted during the device switchover process.

Roles involved in a GR:

- GR Restarter: It is the device that is gracefully restarted.
- GR Helper: It is the device that helps with the GR.
- GR Time: It is the maximum time for GR-Restarters to restart. GR Helper maintains the stability of routes during the period of time.

A dual-controller device can act as a GR Restarter and a GR Helper, while a centralized device can only act as a GR Helper, helping the GR Restarter to complete a GR. When the GR Restarter is in the GR process, the GR Helper maintains the route stability until GR Time timeout. After the GR Helper helps with the GR, it synchronizes route information. During the process, network routes and packet forwarding keep the status before the GR, effectively ensuring the network stability.

The BGP GR relation is set up through OPEN packet negotiation when a connection is set up between neighbors. When the GR Restarter restarts the neighbor, the BGP session will be disconnected, but the routes that are learnt from the neighbor are not deleted. The routes are still normally forwarded in the IP routing table. The routes are labeled with the Stale marks only in the BGP routing table. After the GR is completed, the routes will be refreshed.

The GR Restarter needs to set up a connection with the GR Helper within the maximum allowed time; otherwise, the GR Helper with cancel the maintained GR route and cancel the GR process. After the neighbor is re-connected, the GR Helper needs to receive an update packet with the End-Of-RIB mark from the GR Restarter to complete the GR process; otherwise, the GR route that is not updated will be deleted after the maximum hold time (**stalepath-time**) expires, and then the GR relation is released.

Configuration Condition

Before configuring a BGP GR, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure BGP GR Restarter

Table 790 Configure BGP GR Restarter

Step	Command	Description
Enter the 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*]	Mandatory By default, the BGP device does not enable the GR capability. After enabling GR, the maximum permitted time for the neighbor to re-set up the session is 120s, and the maximum hold time of the GR route is 360s.
Configure advertising the GR-Restarter capability to the neighbor	neighbor { *neighbor-address* | *peer-group-name* } capability graceful-restart	Mandatory By default, do not advertise the GR Restarter capability to the neighbor.

Configure a BGP GR Helper

Table 791 Configure a BGP GR helper

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-

Step	Command	Description
Enable the BGP GR capability.	bgp graceful-restart [restart-time *time* | stalepath-time *time*]	Mandatory. By default, the GR capability is disabled for BGP devices. After the GR capability is enabled, the default maximum allowed time for re-setting up a session with the neighbor is 120s, and the maximum hold time of GR routes is 360s.

6.12.2.8 Configure BGP to Coordinate with BFD

Usually, there are still some intermediate devices between BGP neighbors. When an intermediate device becomes faulty, the BGP session is normal within the hold time, and the link fault caused by the intermediate device cannot be responded to in time. Bidirectional Forwarding Detection (BFD) provides a method for quickly detecting the status of a line between two devices. After BFD is enabled for BGP devices, if a line between two devices becomes faulty, BFD can quickly find the line fault and notifies BGP of the fault. It triggers BGP to quickly disconnect the session and quickly switch over to the backup line, achieving fast switchover of routes.

Configuration Condition

Before configuring BGP to coordinate with BFD, ensure that:

- BGP is enabled.
- BGP neighbors are configured and a session is set up successfully.

Configure EBGP to Coordinate with BFD

The coordination between EBGP and BFD is based on a single-hop BFD session, and BFD session parameters need to be configured in interface mode.

Table 792 Configure EBGP to coordinate with BFD

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure EBGP to coordinate with BFD.	neighbor { *neighbor-address* | *peer-group-name* } fall-over bfd	Mandatory. By default, the BFD function is disabled for a neighbor.
Exit the BGP configuration mode.	exit	-
Enter the interface configuration mode.	interface *interface-name*	-
Configure the minimum receive interval of a BFD session.	bfd min-receive-interval *milliseconds*	Optional. By default, the minimum receive interval of a BFD session is 1000ms.
Configure the minimum transmit interval of the BFD session.	bfd min-transmit-interval *milliseconds*	Optional. By default, the minimum transmit interval of a BFD session is 1000ms.
Configure the multiple of BFD session detection timeout.	bfd multiplier *number*	Optional. By default, the multiple of BFD session detection timeout is 5.

Note

- For the related configuration of BFD, refer to the reliability technology-BFD technical manual and BFD configuration manual.

6.12.2.9 Configure BGP Fast Re-routing

Configuration Conditions

Before configuring BGP to associate with BFD, ensure that:

- Enable the IS-IS protocol.
- Configure the BGP neighbor and the session is connected successfully.

Configure BGP Fast Re-routing

In the BGP network, if the link or device fails, the packet passing the fault point will be dropped or generate the loop and the caused traffic interruption will not recover until the protocol re-converges, which often lasts for several seconds. To reduce the traffic interruption time, you can configure the BGP fast re-routing. Apply the route map to set the backup next hop for the matched route. Once the active link fails, the traffic passing the faulty link will switch to the standby link at once.

Table 793 Configure the BGP fast re-routing

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure fast re-routing	fast-reroute route-map *rtmap-name*	Optional By default, do not enable the fast re-routing function.

Configure auto fast re-routing of BGP	pic	Mandatory By default, do not enable the auto fast re-routing function.

Caution

- After configuring the BGP fast re-routing, you need to re-set BGP and complete the checking and backup of the initial route. Otherwise, it takes effect only for the route learned after configuration.
- For fast re-routing based on route-map, when configuring **set fast-reroute backup-nexthop auto**, the protocol performs auto fast re-routing.
- When using the pic mode, the protocol performs the auto fast re-routing.
- The various modes of enabling the fast re-routing are mutually exclusive.
- After configuring the BGP fast re-routing to apply the route map, set the BGP neighbor as the backup next hop via the **set fast-reroute backup-nexthop** *nexthop-address* command. If configuring the non-BGP neighbor as the backup next hop, you cannot make the fast re-routing function take effect.

6.12.2.10 Configure BGP LS

Configuration Conditions

Before configuring BGP LS, first complete the following task:

- Enable the OSPF protocol
- Set up the OSPF neighbor and configure distribute link-state.

Configure BGP LS

Configure BGP LS to collect the IGP protocol topology information.

Table 794 Configure BGP LS

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP link-state address family	address-family link-state unicast	Optional By default, do not enable the link-state address family.
Activate the LS capability of the BGP neighbor	neighbor { *neighbor-address* | *peer-group-name* } activate	Optional By default, do not activate the LS capability of the BGP neighbor.

6.12.2.11 BGP Monitoring and Maintaining

Table 795 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]	Resets the BGP neighbor.
clear ip bgp [ipv4 unicast | ipv4 multicast] dampening [*ip-address* | *ip-address/mask-length*]	Clears suppressed routes.
clear ip bgp [ipv4 unicast | ipv4 multicast] flap-statistics [*ip-address* | *ip-address/mask-length*]	Clears routing flap statistics.

Command	Description
clear ip bgp { * | *neighbor-address* | *as-number* | peer-group *peer-group-name* | external } [ipv4 unicast | ipv4 multicast | vpnv4 unicast | vrf *vrf-name* | mvpn] { [soft] [in | out] }	Soft resets neighbors.
clear ip bgp { * | *neighbor-address* } in { ecomm | prefix-filter }	Advertises ORF to neighbors.
show ip bgp [vpnv4 { all | vrf *vrf-name* | rd *route-distinguisher* }] [*ip-address* | *ip-address/mask-length*]	Display the routing information in the related BGP address family.
show ip bgp attribute-info	Display the BGP common route attributes.
show ip bgp cidr-only	Display all classful network routes of BGP.
show ip bgp community [*community-number* / *aa:nn* / exact-match / local-AS / no-advertise / no-export]	Display the routes that match the specified community property.
show ip bgp community-info	Display all community property information of BGP.
show ip bgp community-list *community-list-name*	Display the community list that is applied to routes.
show ip bgp [vpnv4 { all | vrf *vrf-name* | rd *route-distinguisher* }] dampening { dampened-paths | flap-statistics | parameters }	Display the details of route attenuation.
show ip bgp filter-list *filter-list-name* [exact-match]	Display the routes that match the AS_PATH filter list.
show ip bgp inconsistent-a	Display the routes that conflict with AS_PATH.

Command	Description
show ip bgp ipv4 vpn-target [*vpn-rt*]	Display the VPN-TARGET route table of BGP
show ip bgp ipv4 vpn-target rt-filter [neighbor *ip-address*]	Display the RT filter table of the BGP neighbor
show ip bgp mvpn { all | vrf *vrf-name* | rd *route-distinguisher* } { all-type | type { 1 [*ip-address*] | 7[*as:source-ip-address:group-ip-address*] } }	Display the route table in the BGP MVPN address family
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*] } }	Display the route information of the specified neighbor in the BGP MVPN address family
show ip bgp mvpn {all | vrf *vrf-name* | rd *route-distinguisher* | neighbors *ip-address* } { all-type | type { 1 | 7 } } { statistics }	Display the route statistics information in the BGP MVPN address family
show ip bgp [vpnv4 { all | vrf *vrf_name* | rd *route-distinguisher* }] neighbors [*ip-address*]	Display the BGP neighbor detailed information
show ip bgp orf ecomm	Display the ORF information of all BGP neighbors.
show ip bgp paths	Display the AS_PATH information of BGP routes.
show ip bgp prefix-list *prefix-list-name*	Display the routes that match the filter list.
show ip bgp quote-regexp *as-path-list-name*	Display the routes that match the AS_PATH list.
show ip bgp regexp *as-path-list-name*	Display the routes that match the AS_PATH list.
show ip bgp route-map *rtmap-name*	Display the routes that match a route map.
show ip bgp scan	Display the BGP scan information.

Command	Description
show ip bgp [vpnv4 { all | vrf *vrf-name* | rd *route-distinguisher* } | mvpn] summary	Display the summary of BGP neighbors.

6.12.3 BGP Typical Configuration Example

6.12.3.1 Configure BGP Basic Functions

Network Requirements

- Set up EBGP neighbors between Device1 and Device2, and set up IBGP neighbors between Device2 and Device3.
- Device1 learns the interface direct route 200.0.0.0/24 of Device3, and Device3 learns the interface direct route 100.0.0.0/24 of Device1.

Network Topology

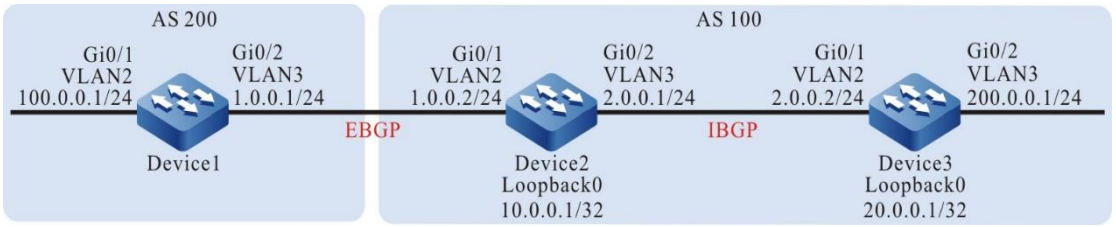


Figure 152 Networking for configuring basic BGP functions

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   20.0.0.1/32 [110/2] via 2.0.0.2, 00:27:09, vlan3
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   10.0.0.1/32 [110/2] via 2.0.0.1, 00:28:13, vlan2
```

According to the queried information, Device2 and Device3 have learnt the routes of the peer loopback interfaces by running OSPF, preparing for setting up IBGP neighbors on the loopback interfaces of Device2 and Device3.

Step 4: Configure BGP.

#Configure Device1.

Set up a direct-connect EBGP peer relation with Device2. Introduce 100.0.0.0/24 to BGP in network mode.

```
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.

Set up a non-direct-connect IBGP peer relation with Device3 through Loopback0, and set the next hop of the advertised route to the local device, and set up a direct-connect EBGP peer relation 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.

Set up a non-direct-connect IBGP peer relation with Device2 through Loopback0. Introduce 200.0.0.0/24 to BGP in network mode.

```
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 flapping, IBGP neighbors are set up through the loopback interfaces, and OSPF need to synchronize the routing information of loopback interfaces between IBGP neighbors.

Step 5: Check the result.

#On Device2, check the BGP neighbor status.

```
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
```

According to the numbers (Number of route prefixes received from neighbors) that are displayed in the State/PfxRcd column, BGP neighbors have been successfully set up between Device 2 and Device 1 and Device2 and Device 3.

#Query the route table of Device1.

```
Device1#show ip route bgp
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, E - IRMP, EX - IRMP external

B   200.0.0.0/24 [20/0] via 1.0.0.2, 00:15:52, vlan3
```

#Query the route table of Device2.

```
Device2#show ip route bgp
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, E - IRMP, EX - IRMP external

B   100.0.0.0/24 [20/0] via 1.0.0.1, 00:14:11, vlan2
B   200.0.0.0/24 [200/0] via 20.0.0.1, 00:17:12, vlan3
```

#Query the route table of Device3.

```
Device3#show ip route bgp
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, E - IRMP, EX - IRMP external

B   100.0.0.0/24 [200/0] via 10.0.0.1, 00:14:50, vlan2
```

Device1 has learnt the interface direct route 200.0.0.0/24 of Device3, and Device3 has learnt the interface direct route 100.0.0.0/24 of Device1.

6.12.3.2 Configure BGP to Redistribute Routes

Network Requirements

- Set up OSPF neighbors between Device3 and Device2, and advertise interface direct-connect route 200.0.0.0/24 to Device2.
- Set up EBGP neighbors between Device1 and Device2, and redistribute the

OSPF route that Device2 learns to BGP and advertise the route to Device1.

Network Topology

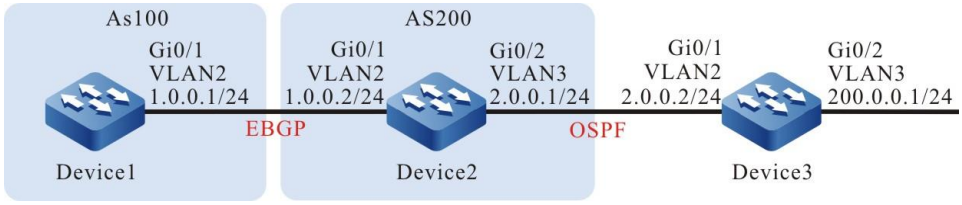


Figure 153 Networking for configuring BGP to redistribute routes

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   200.0.0.0/24 [110/2] via 2.0.0.2, 00:01:45, vlan3
```

According to the route table, Device2 has learnt the OSPF route 200.0.0.0/24 that has been 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 100
Device2(config-bgp)#exit
```

#On Device2, check the BGP neighbor status.

```
Device2#show ip bgp summary
BGP router identifier 2.0.0.1, 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   200       2       2        2    0    0 00:00:42        0
```

BGP neighbors have been successfully set up between Device2 and Device1.

Step 5: Configure BGP to redistribute the OSPF route.

#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 route 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
[0]*> 2.0.0.0/24       0.0.0.0              1       32768 ?
[0]*> 200.0.0.0/24     2.0.0.2              2       32768 ?
```

According to the queried information, OSPF routes have been successfully redistributed to BGP.

#Query the route table of Device1.

```
Device1#show ip route bgp
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, E - IRMP, EX - IRMP external

B   2.0.0.0/24 [20/1] via 1.0.0.2, 00:06:14, vlan2
B   200.0.0.0/24 [20/2] via 1.0.0.2, 00:06:14, vlan2
```

According to the queried information, Device1 has successfully learnt 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 redistribute routes between different routing protocols. If route redistribution must be configured, you are required to configure route control policies such as route filtering and filtration summary on the AS boundary routers to prevent routing loops.

---

6. 12. 3. 3 Configure BGP Community Properties

Network Requirements

- Set up EBGP neighbors between Device1 and Device2.
- Device1 introduces two direct-connect routes 100.0.0.0/24 and 200.0.0.0/24 to BGP in network mode, and set different community properties for two routes that are advertised to Device2.

- When Device2 receives routes from Device1, it applies community properties in the incoming direction of a neighbor to filter route 100.0.0.0/24 and allow route 200.0.0.0/24.

Network Topology

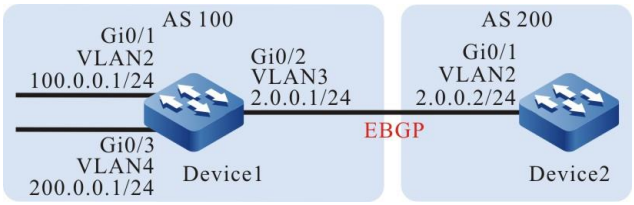


Figure 154 Networking for configuring BGP community properties

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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
```

#On Device1, check the BGP neighbor status.

```
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 00:00:04        0
```

BGP neighbors have been successfully set up between Device1 and Device2.

#Query the route table of Device2.

```
Device2#show ip route bgp
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, E - IRMP, EX - IRMP external

B   100.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
B   200.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
```

According to the queried information, Device2 has successfully learnt routes 100.0.0.0/24 and 200.0.0.0/24.

Step 4: Configure the ACL and routing policy, and set BGP community properties.

#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)#commit
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)#commit
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 properties for routes 100.0.0.0/24 and 200.0.0.0/24 respectively by configuring an ACL and routing policy.

Step 5: Configure a routing 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 route table of Device2.

```
Device2#show ip bgp 100.0.0.0
BGP route 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 route 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: 00:01:10 ago
```

According to the BGP route table of Device2, the community property of route 100.0.0.0/24 is set to 100:1, and the community properties of route 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 route table of Device2.

```
Device2#show ip route bgp
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, E - IRMP, EX - IRMP external

B   200.0.0.0/24 [20/0] via 2.0.0.1, 00:00:53, vlan2
```

According to the BGP route table of Device2, route 100.0.0.0/24 has been filtered in the incoming direction, and route 200.0.0.0/24 has been allowed.

Note

- After a routing policy is configured on the peer, the BGP must be reset to make the configuration take effect.
- You must configure the **send-community** command to advertise the community property to the peer.

6.12.3.4 Configure BGP Route Reflector

Network Requirements

- Set up EBGP neighbors between Device3 and Device4, and configure Device4 to advertise route 100.0.0.0/24.
- Set up IBGP neighbors between Device2 and Device3 and between Device2 and Device1 respectively. On Device2, configure Route Reflectors (RRs), and configure Device1 and Device3 as clients, so that Device1 can learn route 100.0.0.0/24 that is advertised by Device4.

Network Topology

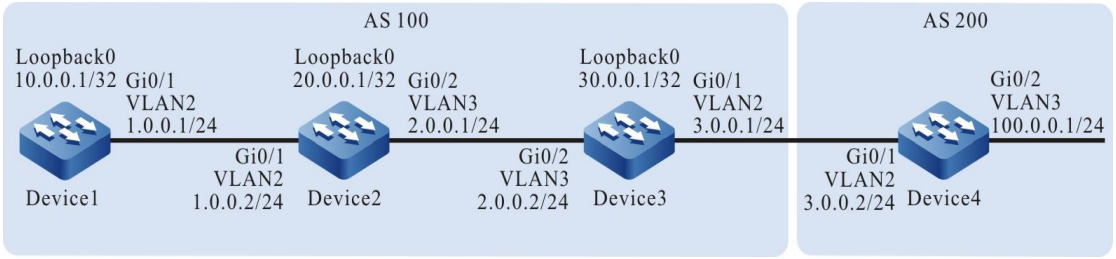


Figure 155 Networking for configuring a BGP route reflector

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

O   2.0.0.0/24 [110/2] via 1.0.0.2, 01:12:00, vlan2
O   20.0.0.1/32 [110/2] via 1.0.0.2, 01:11:47, vlan2
O   30.0.0.1/32 [110/3] via 1.0.0.2, 01:07:47, vlan2
```

#Query the route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   10.0.0.1/32 [110/2] via 1.0.0.1, 01:13:02, vlan2
O   30.0.0.1/32 [110/2] via 2.0.0.2, 01:08:58, vlan3
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   1.0.0.0/24 [110/2] via 2.0.0.1, 01:10:04, vlan2
O   10.0.0.1/32 [110/3] via 2.0.0.1, 01:10:04, vlan2
O   20.0.0.1/32 [110/2] via 2.0.0.1, 01:10:04, vlan2
```

According to the route table, Device1, Device2, and Device3 have learnt the routes of the loopback interfaces of each other.

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
```

#On Device2, check the BGP neighbor status.

```
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 00:03:01        0
30.0.0.1        4   100       9       9        1    0    0 00:02:41        1
```

#On Device4, check the BGP neighbor status.

```
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
```

According to the queried information, BGP neighbors have been set up between the devices.

#Query the BGP route 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 route 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 route 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 route table, Device2 and Device3 have learnt route 100.0.0.0/24, and Device2 has not advertised the route to Device1.

Step 5: Configure a 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, Device1 and Device3 have been configured as the RR clients.

Step 6: Check the result.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   100.0.0.0/24 [200/0] via 30.0.0.1, 00:01:40, vlan2
```

On BGP of Device2, Device1 and Device3 have been configured as the RR clients, and Device2 has successfully reflects route 100.0.0.0/24 to RR client Device1.

Note

- If you configure a peer as a RR client, the device and the neighbors of the peer will be reset.

6.12.3.5 Configure BGP Route Summary

Network Requirements

- Set up OSPF neighbors between Device1 and Device3, and configure Device3 to advertise routes 100.1.0.0/24 and 100.2.0.0/24 to Device1.
- Set up EBGP neighbors between Device1 and Device2.
- On Device1, aggregate routes 100.1.0.0/24 and 100.2.0.0/24 into route 100.0.0.0/14 and advertise the aggregated route to Device2.

Network Topology

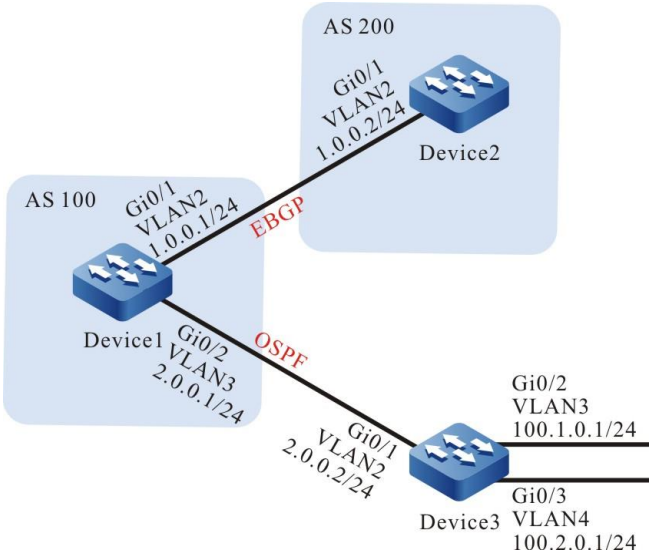


Figure 156 Networking for configuring BGP route summary

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF.

#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 route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

O   100.1.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
O   100.2.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
```

According to the route table, Device1 has learnt 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
```

#On Device1, check the BGP neighbor status.

```
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 00:00:42        0
```

BGP neighbors have been successfully set up between Device1 and Device2.

Step 5: Configure BGP route summary.

Two solutions are available to satisfy network requirements.

Solution 1: Configure an aggregated static route that is targeted at null0 to introduce the aggregated static route 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 route 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
```

The aggregated route 100.0.0.0/14 has been generated in the BGP route table of Device1.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

Device2 has successfully learnt the aggregated route 100.0.0.0/14 that has been advertised by Device1.

Solution 2: First introduce common routes into BGP, and then run the **aggregate-address** command to aggregate the routes.

#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 route 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
```

The aggregated route 100.0.0.0/14 has been generated in the BGP route table of Device1.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external
B   100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

Device2 has successfully learnt the aggregated route 100.0.0.0/14 that has been advertised by Device1.

Note

- When the **aggregate-address** command is used to aggregate routes, if the extended command **summary-only** is configured, the device advertises

only the aggregated route; otherwise, both common routes and aggregated routes are advertised.

6.12.3.6 Configure the BGP Route Selection Priority

Network Requirements

- 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.
- Device1 advertises two routes 55.0.0.0/24 and 65.0.0.0/24 to Device4, and Device4 advertises two routes 75.0.0.0/24 and 85.0.0.0/24 to Device1.
- Modify the Local-preference property of routes on Device2 and Device3 so that Device1 selects route 75.0.0.0/24 advertised by Device2 and route 85.0.0.0/24 advertised by Device3 with priority.
- Modify the MED property of routes on Device2 and Device3 so that Device4 selects route 55.0.0.0/24 advertised by Device2 and route 65.0.0.0/24 advertised by Device3 with priority.

Network Topology

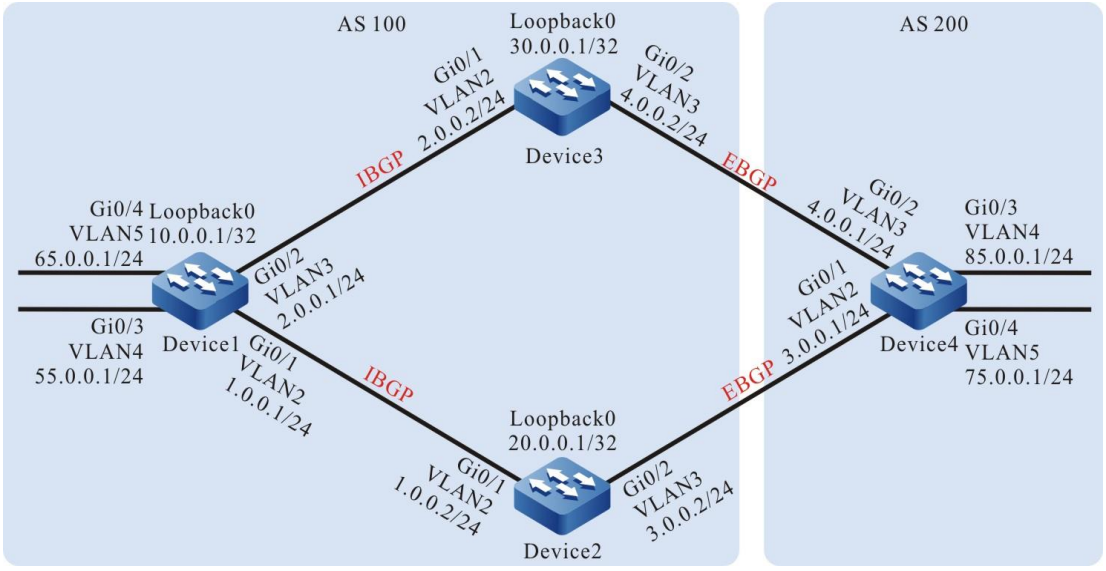


Figure 157 Networking for configuring the BGP route selection priority

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

O   20.0.0.1/32 [110/2] via 1.0.0.2, 00:03:15, vlan2
O   30.0.0.1/32 [110/2] via 2.0.0.2, 00:01:40, vlan3
```

#Query the route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   2.0.0.0/24 [110/2] via 1.0.0.1, 00:03:54, vlan2
O   10.0.0.1/32 [110/2] via 1.0.0.1, 00:03:54, vlan2
O   30.0.0.1/32 [110/3] via 1.0.0.1, 00:02:14, vlan2
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   1.0.0.0/24 [110/2] via 2.0.0.1, 00:02:35, vlan2
O   10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:35, vlan2
O   20.0.0.1/32 [110/3] via 2.0.0.1, 00:02:35, vlan2
```

According to the route table, Device1, Device2, and Device3 have learnt the routes of the loopback interfaces of each other.

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
```

#On Device1, check the BGP neighbor status.

```
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 00:03:59        2
```

#On Device4, check the BGP neighbor status.

```
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 00:02:24        2
4.0.0.2         4   100       6       5        2    0    0 00:02:24        2
```

IBGP neighbors have been set up between Device1 and Device2 and between Device2 and Device3, and EBGP neighbors have been set up between Device4 and Device2 and between Device4 and Device3.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   75.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
B   85.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
```

According to the route table, both route 75.0.0.0/24 and route 85.0.0.0/24 of Device1 select Device2 as the next-hop device.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   55.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3
B   65.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3
```

According to the route table, both route 55.0.0.0/24 and route 65.0.0.0/24 of Device4 select Device3 as the next-hop device.

Step 5: Configure an ACL and routing policy to 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)#commit
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)#commit
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
```

On Device2, configure a routing policy to set local-preference of route 75.0.0.0/24 to 110, and set metric of 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)#commit
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)#commit
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
```

On Device3, configure a routing policy to set local-preference of route 85.0.0.0/24 to 110, and set metric of route 55.0.0.0/24 to 100.

Note

- In configuring a routing 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 a routing 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
```

On Device2, configure the outgoing direction of neighbor 10.0.0.1 to modify local-preference of route 75.0.0.0/24, and configure the outgoing direction of neighbor 3.0.0.1 to modify metric of route 65.0.0.0/24.

#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
```

On Device3, configure the outgoing direction of neighbor 10.0.0.1 to modify local-preference of route 85.0.0.0/24, and configure the outgoing direction of neighbor 4.0.0.1 to modify metric of route 55.0.0.0/24.

After a routing policy is configured on the peer, the BGP must be reset to make the configuration take effect.

Step 7: Check the result.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   75.0.0.0/24 [200/0] via 20.0.0.1, 00:01:34, vlan2
B   85.0.0.0/24 [200/0] via 30.0.0.1, 00:00:51, vlan3
```

According to the route table, local-preference of routes 75.0.0.0/24 and 85.0.0.0/24 is modified successfully, and Device1 select route 75.0.0.0/24 that is advertised by Device2 and route 85.0.0.0/24 that is advertised by Device3 with priority.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   55.0.0.0/24 [20/0] via 3.0.0.2, 00:15:02, vlan2
B   65.0.0.0/24 [20/0] via 4.0.0.2, 00:14:55, vlan3
```

According to the route table, metric of routes 55.0.0.0/24 and 65.0.0.0/24 is modified successfully, and Device4 select route 55.0.0.0/24 that is advertised by Device2 and route 65.0.0.0/24 that is advertised by Device3 with priority.

Note

- A routing policy can be used in the outgoing direction of route advertisement, and it can also be used in the incoming direction of route receiving.

6.12.3.7 Configure BGP Confederation

Network Requirements

- Device2, Device3, Device4, and Device5 are in the same BGP AS 200. To reduce the number of IBGP full connections, they are divided into two different ASs in one BGP confederation.
- Set up EBGP neighbors between Device1 and Device2, and advertise route 100.0.0.0/24 to AS 200.

Network Topology

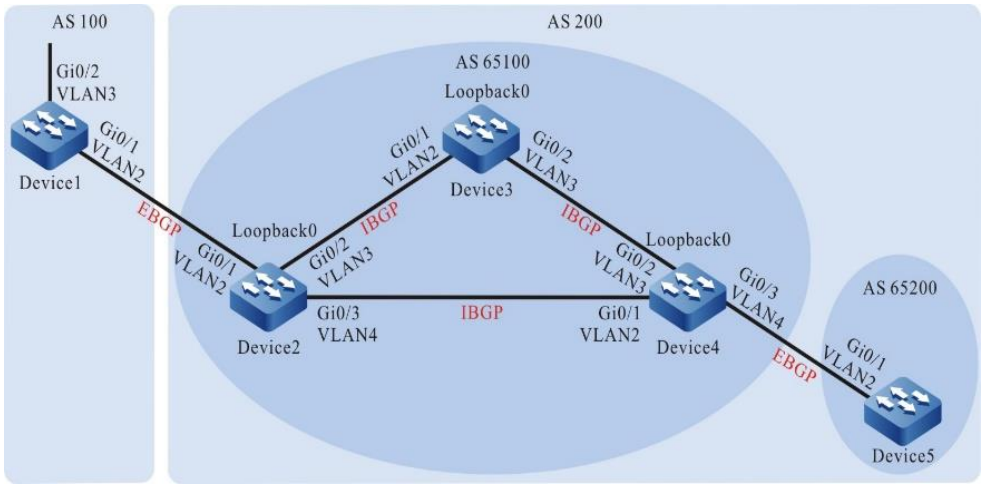


Figure 158 Networking for configuring a BGP confederation

Device	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
	Gi0/2	3	4.0.0.2/24
	Gi0/3	4	5.0.0.1/24
	Loopback0		40.0.0.1/32

Device	Interface	VLAN	IP Address
Device5	Gi0/1	2	5.0.0.2/24

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   4.0.0.0/24 [110/2] via 2.0.0.1, 00:02:42, vlan3
                [110/2] via 3.0.0.1, 00:02:11, vlan4
O   30.0.0.1/32 [110/2] via 2.0.0.1, 00:02:32, vlan3
O   40.0.0.1/32 [110/2] via 3.0.0.1, 00:02:05, vlan4
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   3.0.0.0/24 [110/2] via 2.0.0.2, 00:03:24, vlan2
                [110/2] via 4.0.0.2, 00:02:38, vlan3
O   20.0.0.1/32 [110/2] via 2.0.0.2, 00:03:24, vlan2
O   40.0.0.1/32 [110/2] via 4.0.0.2, 00:02:38, vlan3
```

#Query the route table of Device4.

```
Device4#show ip route ospf
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, E - IRMP, EX - IRMP external

O   2.0.0.0/24 [110/2] via 3.0.0.2, 00:03:42, vlan2
                [110/2] via 4.0.0.1, 00:03:42, vlan3
O   20.0.0.1/32 [110/2] via 3.0.0.2, 00:03:42, vlan2
O   30.0.0.1/32 [110/2] via 4.0.0.1, 00:03:42, vlan3
```

#Query the route table of Device5.

```
Device5#show ip route ospf
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, E - IRMP, EX - IRMP external

O   2.0.0.0/24 [110/3] via 5.0.0.1, 00:00:03, vlan2
```

```
O   3.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
O   4.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
O   20.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
O   30.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
O   40.0.0.1/32 [110/2] via 5.0.0.1, 00:00:03, vlan2
```

According to the route table, Device2, Device3, and Device4 have learnt the routes of the loopback interfaces of each other.

Step 4: Configure BGP connections in a confederation.

Configure IBGP connections in a 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 EBGP connections in a 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
```

#On Device4, check the BGP neighbor status.

```
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 00:05:39        0
```

IBGP neighbors have been set up between Device4 and Device2 and between Device4 and Device3, and EBGP neighbors have been set up between Device4 and Device5.

Step 5: Configure a BGP confederation.

#Configure Device1.

Configure an EBGP peer. The AS number of the peer is 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 to 200, and configure an EBGP peer. The peer AS number is 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 the BGP confederation 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 to 200, and configure the confederation to contain 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 to 200, and configure the confederation to contain 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.

#On Device1, check the BGP neighbor status.

```
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
```

EBGP neighbors have been successfully set up between Device1 and Device2.

#On Device5, query the route information.

```
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 bgp
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, E - IRMP, EX - IRMP external
B   100.0.0.0/24 [200/0] via 20.0.0.1, 00:00:38, vlan2
```

Device5 has successfully learnt route 100.0.0.0/24, and the next-hop property of the route keeps unchanged while the route is transmitted in the confederation. Device2, Device3, Device4, and Device5 belong to the same confederation, and full connections are not required. Device5 obtains external route information through Device4.

6.12.3.8 Configure BGP to Coordinate with BFD

Network Requirements

- Set up EBGP neighbors between Device1 and Device2 and between Device1 and Device3, and set up IBGP neighbors between Device2 and Device3.
- Device1 learns EBGP route 3.0.0.0/24 both from Device2 and Device3, and Device1 selects to forward data to the network segment 3.0.0.0/24 through Device2.
- On Device1 and Device2, configure EBGP to coordinate with BFD. When the line between Device1 and Device2 becomes faulty, BFD can quickly detect the fault and notify BGP of the fault. Then Device1 selects to forward data to network segment 3.0.0.0/24 through Device3.

Network Topology

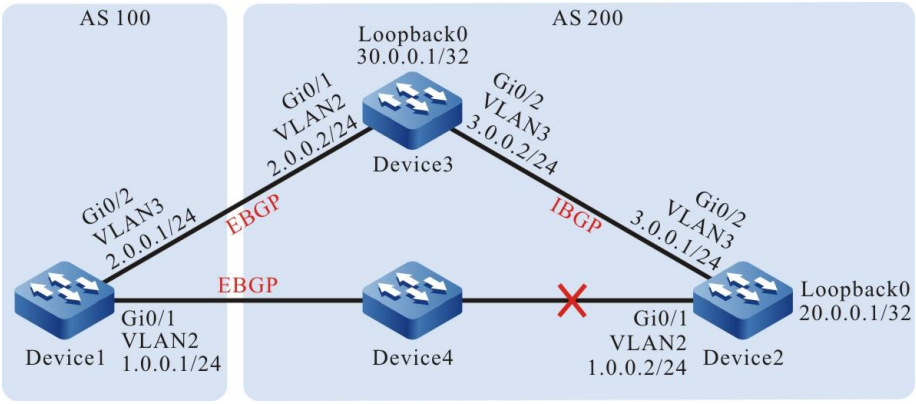


Figure 159 Networking for configuring BGP to coordinate with BFD

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external
```

```
O   30.0.0.1/32 [110/2] via 3.0.0.2, 00:02:26, vlan3
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   20.0.0.1/32 [110/2] via 3.0.0.1, 00:03:38, vlan3
```

According to the route table, Device2 and Device3 have learnt the routes of the loopback interfaces of each other.

Step 4: Configure an ACL and routing policy to set metric of a route.

#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)#commit
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
```

The routing policy that is configured on Device1 sets the metric of route 3.0.0.0/24 to 50.

Step 5 Configure BGP, and configure Device1 with a routing policy.

#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
```

After a routing policy is configured on the peer, the BGP must be reset to make the configuration take effect.

#On Device1, check the BGP neighbor status.

```
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 00:01:32        1
2.0.0.2         4   200       2       2        2    0    0 00:01:43        1
```

#On Device2, check the BGP neighbor status.

```
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 00:02:52        0
30.0.0.1        4   200       3       3        2    0    0 00:02:45        1
```

BGP neighbors between Device1, Device2, and Device3 have been set up successfully.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   3.0.0.0/24 [20/0] via 1.0.0.2, 00:07:19, vlan2
```

According to the route table, route 3.0.0.0/24 of Device1 selects Device2 as the next-hop device.

Step 6: Configure BGP to coordinate 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
```

BFD is enabled between EBGP neighbors Device1 and Device2, and the minimum transmit interval, minimum receive interval, and detection timeout multiple of the BFD control packets have been modified.

Step 7: Check the result.

#On Device1, query the BFD session status.

```
Device1#show bfd session
OurAddr          NeighAddr          LD/RD          State      Holddown      interface
1.0.0.1          1.0.0.2            2/2            UP         2000          vlan2
```

On Device1, the BFD status is up, and the holddown time is negotiated to be 2000ms.

#If the line between Device1 and Device2 becomes faulty, the route can quickly switch over to the backup line.

#Query the route 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 bgp
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, E - IRMP, EX - IRMP external

B   3.0.0.0/24 [20/50] via 2.0.0.2, 00:00:05, vlan3
```

The next hop of route 3.0.0.0/24 is Device3.

6.12.3.9 Configure BGP Fast Re-routing

Network Requirements

- All devices configure the BGP protocol.
- Device1 learns the ISIS route 192.168.1.1/32 from Device2 and Device3 at the same time. Device1 first uses the line with Device3 to forward the packet. Similarly, Device3 learns the BGP route 100.1.1.1/32 from Device1 and Device2 at the same time. Device3 first uses the line with Device1 to

forward the packet.

- Device1 and Device3 enable the BGP fast re-routing. After the line between Device1 and Device3 fails, the service can switch to Device2 for communication fast.

Network Topology

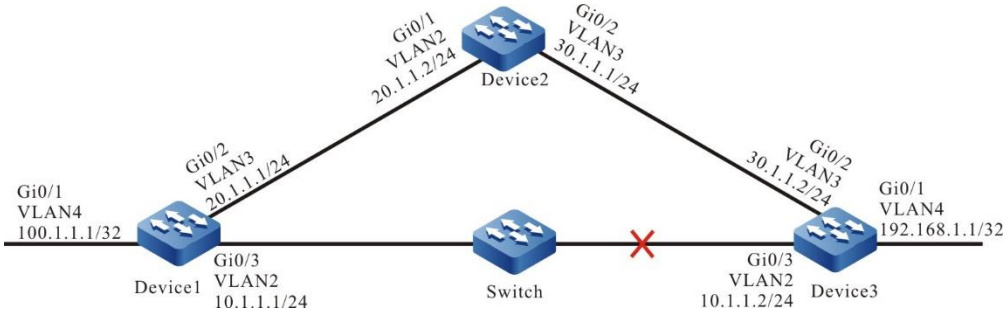


Figure 160 Networking for configuring BGP fast re-routing

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IP addresses of the interfaces. (Omitted)

Step 2: Configure BGP.

#Configure Device1 to set up the BGP neighbor with Device2, Device3, and the weight of the neighbor route with Device3 is 100.

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 10.1.1.2 remote-as 300
Device1(config-bgp)#neighbor 10.1.1.2 weight 100
Device1(config-bgp)#neighbor 20.1.1.2 remote-as 200
Device1(config-bgp)#network 100.1.1.1 255.255.255.255
Device1(config-bgp)#exit
```

#Configure Device2 to set up the BGP neighbor with Device1, Device3.

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 20.1.1.1 remote-as 100
Device2(config-bgp)#neighbor 30.1.1.2 remote-as 300
Device2(config-bgp)#exit
```

#Configure Device3 to set up the BGP neighbor with Device1, Device2, and the weight of the neighbor route with Device1 is 100.

```
Device3#configure terminal
Device3(config)#router bgp 300
Device3(config-bgp)#neighbor 10.1.1.1 remote-as 100
Device3(config-bgp)#neighbor 10.1.1.1 weight 100
Device3(config-bgp)#neighbor 30.1.1.1 remote-as 200
Device3(config-bgp)#network 195.168.1.1 255.255.255.255
Device3(config-bgp)#exit
```

Step 3: Configure the route policy.

#Configure Device1: configure route-map to call the ACL only matching 192.168.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface gigabitethernet1 and the next-hop address is 20.1.1.2.

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 192.168.1.1 0.0.0.0
Device1(config-std-nacl)#exit
Device1(config)#route-map ipfrr_bgp
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set fast-reroute backup-nexthop 20.1.1.2
Device1(config-route-map)#exit
```

#Configure Device3: configure route-map to call the ACL only matching 100.1.1.1/32, while the other network is filtered. The route matching the match rule applies the backup next-hop interface gigabitethernet1 and the next-hop address is 30.1.1.1.

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 100.1.1.1 0.0.0.0
Device3(config-std-nacl)#exit
Device3(config)#route-map ipfrr_bgp
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set fast-reroute backup-nexthop 30.1.1.1
Device3(config-route-map)#exit
```

Step 4: Configure the fast re-routing.

#Configure Device1 to enable the BGP fast re-routing.

```
Device1(config)#router bgp 100
Device1(config-bgp)#fast-reroute route-map ipfrr_bgp
Device1(config-bgp)#exit
```

#Configure Device3 to enable the BGP fast re-routing.

```
Device3(config)#router bgp 300
Device3(config-bgp)#fast-reroute route-map ipfrr_bgp
Device3(config-bgp)#exit
```

Step 5: Check the result.

#View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.1.1.0/24 is directly connected, 00:45:55, vlan2
L   10.1.1.1/32 is directly connected, 00:45:55, vlan2
C   20.1.1.0/24 is directly connected, 01:29:32, vlan3
L   20.1.1.1/32 is directly connected, 01:29:32, vlan3
C   127.0.0.0/8 is directly connected, 01:36:07, lo0
L   127.0.0.1/32 is directly connected, 01:36:07, lo0
LC 100.1.1.1/32 is directly connected, 01:35:18, vlan 4
B   192.168.1.1/32 [20/0] via 10.1.1.2, 00:04:40, vlan2
```

#View the fast re-route table of Device1 and you can see the route of the network 192.168.1.1/32 and the next-hop interface is vlan3.

```
Device1#show ip frr 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, E - IRMP, EX - IRMP external
B   192.168.1.1/32 [20/0] via 20.1.1.2, 00:00:02, vlan3
```

#View the backup next-hop information of Device1 and the backup interface of the fast re-routing is vlan3.

```
Device1#show nexthop frr detail
Index               : 108
Type                : FRR
Reference Count     : 1
Active Path         : master
Nexthop Address     : 10.1.1.2
Interface           : vlan2
```

```
Interface Vrf          : global
Channel ID             : 19
Link Header Length     : 18
Link Header            : 01017abc662b20120101010181000010800
Action                 : FORWORDING
Slot                   : 0
BK Nexthop Address     : 20.1.1.2
BK Interface           : vlan3
BK Interface Vrf       : global
BK Channel ID          : 20
BK Link Header Length  : 18
BK Link Header         : 01017a45544920120101010281000020800
BK Action              : FORWORDING
BK Slot                : 0


Total 1 entries.
```

#After the line between Device1 and Device3 fails, the system can fast detect and switch to Device2 for communication. View the route table and fast re-route table of Device1. The egress interface to the destination network 192.168.1.1/32 in the route table is switched to the backup interface vlan3.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
C   10.1.1.0/24 is directly connected, 00:45:55, vlan2
L   10.1.1.1/32 is directly connected, 00:45:55, vlan2
C   20.1.1.0/24 is directly connected, 01:29:32, vlan3
L   20.1.1.1/32 is directly connected, 01:29:32, vlan3
C   127.0.0.0/8 is directly connected, 01:36:07, lo0
L   127.0.0.1.32 is directly connected, 01:36:07, lo0
LC  100.1.1.1/32 is directly connected, 01:35:18, vlan 4
B   192.168.1.1/32 [20/0] via 20.1.1.2, 00:00:40, vlan3
```

The processing mode of Device3 is similar to Device1.

6.12.3.10 Configure BGP-LS Basic Function

Network Requirements

- Device1 establishes an OSPF neighbor with Device2, and Device1 notifies Device2 of the loopback route.

- Device3 establishes an OSPF neighbor with Device2, and Device3 notifies Device2 of the loopback route.
- Device2 establishes a BGP-LS neighbor with Device4, and Device2 notifies Device4 of the BGP-LS route.

Network Topology

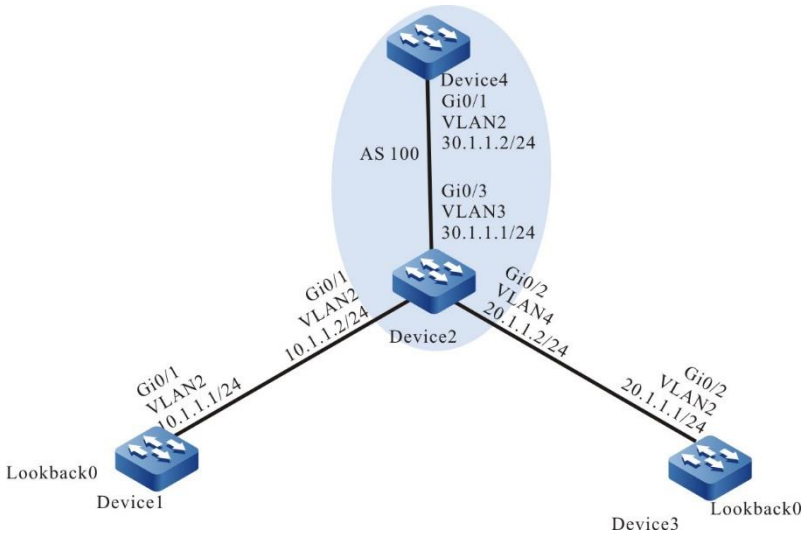


Figure 161 Networking of configuring BGP-LS basic functions

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IP addresses of the interfaces. (Omitted)

Step 2: Configure OSPF.

#Configure Device1, and Device1 and Device2 set up the OSPF neighbor of the backbone area.

```
Device1#configure terminal
Device1(config)#router ospf 65535
Device1(config-ospf)#router-id 100.1.1.1
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
```

```
Device2(config)#router ospf 65535
Device2(config-ospf)#router-id 100.1.1.2
Device2(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 10
Device2(config-ospf)#exit
```

#Configure Device3, and Device3 and Device2 set up the OSPF neighbor of non-backbone area.

```
Device3#configure terminal
Device3(config)#router ospf 65535
Device3(config-ospf)#router-id 100.1.1.3
Device2(config-ospf)#network 20.1.1.0 0.0.0.255 area 10
Device3(config-ospf)#network 3.3.3.3 0.0.0.0 area 10
Device3(config-ospf)#exit
```

Step 3: Configure BGP.

#On Device2, configure BGP, and activate the BGP-LS capability of the neighbor.

```
Device2#configure terminal
Device2(config)#router bgp 65535
Device2(config-bgp)#bgp router-id 100.1.1.2
Device2(config-bgp)#neighbor 30.1.1.2 remote-as 65535
Device2(config-bgp)#address-family link-state unicast
Device2(config-bgp-af)#neighbor 30.1.1.2 activate
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#On Device4, configure BGP, and activate the BGP-LS capability of the neighbor.

```
Device4#configure terminal
Device4(config)#router bgp 65535
Device4(config-bgp)#bgp router-id 100.1.1.4
Device4(config-bgp)#neighbor 30.1.1.1 remote-as 65535
Device4(config-bgp)#address-family link-state unicast
Device4(config-bgp-af)#neighbor 30.1.1.1 activate
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

Step 4: Configure OSPF to import the IGP topology information.

#On Device2, configure importing the IGP topology information in the OSPF address family.

```
Device2(config)#router ospf 65535
```

```
Device2(config-ospf)#distribute link-state
Device2(config-ospf)#exit
```

Step 5: Check the result.

#View the generated IGP node topology information of Device2.

```
Device2#show ip ospf 65535 link-state node
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route

 N 100.1.1.1: [area:0.0.0.0] [DR:-] flags:0x0
 N 100.1.1.2: [area:0.0.0.0] [DR:-] flags:0x10 ABR
 N 100.1.1.2: [area:0.0.0.0] [DR:10.1.1.2] flags:0x10 ABR
 N 100.1.1.2: [area:0.0.0.10] [DR:-] flags:0x10 ABR
 N 100.1.1.3: [area:0.0.0.10] [DR:-] flags:0x0
 N 100.1.1.3: [area:0.0.0.10] [DR:20.1.1.2] flags:0x0

Node route total number 6
```

#View the generated IGP link topology information of Device2.

```
Device2#show ip ospf 65535 link-state link
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route

 L [100.1.1.1:10.1.1.1][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
 L [100.1.1.2:10.1.1.2][100.1.1.1:10.1.1.1][area:0.0.0.0][DR:10.1.1.2] metric:1
 L [100.1.1.2:10.1.1.2][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
 L [100.1.1.2:10.1.1.2][100.1.1.2:10.1.1.2][area:0.0.0.0][DR:10.1.1.2] metric:1
 L [100.1.1.2:20.1.1.1][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1
 L [100.1.1.3:20.1.1.2][100.1.1.2:20.1.1.1][area:0.0.0.10][DR:20.1.1.2] metric:1
 L [100.1.1.3:20.1.1.2][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1
 L [100.1.1.3:20.1.1.2][100.1.1.3:20.1.1.2][area:0.0.0.10][DR:20.1.1.2] metric:1

Link route total number 8
```

#View the generated IGP prefix topology information of Device2.

```
Device2#show ip ospf 65535 link-state prefix
OSPF process 65535:
OSPF-LS local link state route:
Codes: N - Node route, L - Link route, P - Prefix route
```

P 100.1.1.1:[1.1.1.1/32][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.1:[10.1.1.0/24][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[10.1.1.0/24][area:0.0.0.0] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[20.1.1.0/24][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.3:[3.3.3.3/32][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.3:[20.1.1.0/24][area:0.0.0.10] type:1 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[3.3.3.3/32][area:0.0.0.0] type:2 Fwd:0.0.0.0 metric:2
P 100.1.1.2:[20.1.1.0/24][area:0.0.0.0] type:2 Fwd:0.0.0.0 metric:1
P 100.1.1.2:[1.1.1.1/32][area:0.0.0.10] type:2 Fwd:0.0.0.0 metric:2
P 100.1.1.2:[10.1.1.0/24][area:0.0.0.10] type:2 Fwd:0.0.0.0 metric:1

Prefix route total number 10

#View the generated BGP-LS node route of Device2.

```
Device2#show bgp link-state unicast type node
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
              I Identifier, N local node, R remote node, L link, P prefix,
              L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
              a area-ID, l link-ID, t topology-ID, s ISO-ID,
              c confed-ID/ASN, b bgp-identifier, r router-ID,
              i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
              d designated router address
 Node Routes:
    Network          Next Hop            Metric     LocPrf Weight Path
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]]
                     0.0.0.0                  0          32768 i
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]]
                     0.0.0.0                  0          32768 i
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]]
                     0.0.0.0                  0          32768 i
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]]
                     0.0.0.0                  0          32768 i
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]]
                     0.0.0.0                  0          32768 i
[0]*> [V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]]
                     0.0.0.0                  0          32768 i
```

#View the generated BGP-LS link route of Device2.

```
Device2#show bgp link-state unicast type link
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
I Identifier, N local node, R remote node, L link, P prefix,
L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
a area-ID, l link-ID, t topology-ID, s ISO-ID,
c confed-ID/ASN, b bgp-identifier, r router-ID,
i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
d designated router address
Link Routes:
Network Next Hop Metric LocPrf Weight Path
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.1][n10.1.1.2]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.2][n10.1.1.2]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.1][n20.1.1.2]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.2][n20.1.1.2]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][L[i10.1.1.2][n10.1.1.1]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][L[i10.1.1.2][n10.1.1.2]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][L[i20.1.1.2][n20.1.1.1]]
0.0.0.0 0 32768 i
[0]*>
[E][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][L[i20.1.1.2][n20.1.1.2]]
0.0.0.0 0 32768 i

Total number of prefixes 8

#View the generated BGP-LS prefix route of Device2.

Device2#show bgp link-state unicast type prefix4
BGP local router ID is 100.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale

```
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
        I Identifier, N local node, R remote node, L link, P prefix,
        L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
        a area-ID, l link-ID, t topology-ID, s ISO-ID,
        c confed-ID/ASN, b bgp-identifier, r router-ID,
        i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
        d designated router address
 Prefix4 Routes:
    Network          Next Hop          Metric     LocPrf Weight Path
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p10.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p1.1.1.1/32]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x01][p10.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p20.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p3.3.3.3/32]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x01][p20.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p10.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p1.1.1.1/32]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p20.1.1.0/24]]
                    0.0.0.0                0          32768 i
[0]*> [T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p3.3.3.3/32]]
                    0.0.0.0                0          32768 i

Total number of prefixes 10
```

#On Device4, view the BGP-LS route received from Device2.

```
Device4#show bgp link-state unicast all-type
BGP local router ID is 100.1.1.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
        S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Prefix codes: E link, V node, T IP reachable route, u/U unknown,
        I Identifier, N local node, R remote node, L link, P prefix,
        L1/L2 ISIS level-1/level-2, O OSPF, D direct, S static,
        a area-ID, l link-ID, t topology-ID, s ISO-ID,
        c confed-ID/ASN, b bgp-identifier, r router-ID,
        i if-address, n nbr-address, o OSPF Route-type, p IP-prefix
```

d designated router address

Node Routes:

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]]					
	30.1.1.1	0	100	0	i
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]]					
	30.1.1.1	0	100	0	i
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[V][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]]					
	30.1.1.1	0	100	0	i

Link Routes:

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.1][n10.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][L[i10.1.1.2][n10.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.1][n20.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][L[i20.1.1.2][n20.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][L[i10.1.1.2][n10.1.1.1]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2d10.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][L[i10.1.1.2][n10.1.1.2]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][L[i20.1.1.2][n20.1.1.1]]					
	30.1.1.1	0	100	0	i
[B]*>i[E][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3d20.1.1.2]][R[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][L[i20.1.1.2][n20.1.1.2]]					
	30.1.1.1	0	100	0	i

Prefix4 Routes:

Network	Next Hop	Metric	LocPrf	Weight	Path
[B]*>i[T][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p10.1.1.0/24]]					
	30.1.1.1	0	100	0	i
[B]*>i[T][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.1]][P[o0x01][p1.1.1.1/32]]					
	30.1.1.1	0	100	0	i
[B]*>i[T][0][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x01][p10.1.1.0/24]]					

```
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p20.1.1.0/24]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.0][r100.1.1.2]][P[o0x02][p3.3.3.3/32]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x01][p20.1.1.0/24]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p10.1.1.0/24]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.2]][P[o0x02][p1.1.1.1/32]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p20.1.1.0/24]]
                    30.1.1.1             0      100      0 i
[B]*>i[T][O][I0x0][N[c65535][b100.1.1.2][a0.0.0.10][r100.1.1.3]][P[o0x01][p3.3.3.3/32]]
                    30.1.1.1             0      100      0 i

Total number of prefixes 2
```

6.13 IPv6 BGP

6.13.1 Overview

IPv6 BGP (BGP4 +) is extended from BGP-4. BGP-4 can only manage IPv4 routing information. 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 IPv6 network layer protocol information into NLRI (Network Layer Reachability Information) and NEXT_HOP attributes. The two NLRI attributes introduced in IPv6 BGP are:

MP_REACH_NLRI: Multiprotocol Reachable NLRI, used to release the reachable route and next-hop information

MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI, used to cancel the unreachable route

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 uses the multi-protocol extension attributes of BGP to realize the application in IPv6 network. The original message mechanism and routing mechanism

of BGP the protocol do not change.

6.13.2 IPv6 BGP Function Configuration

Table 796 IPv6 BGP function list

Configuration Tasks	
Configure an IPv6 BGP neighbor.	Configure an IBGP neighbor.
	Configure an EBGP neighbor.
	Configure a BGP passive neighbor.
	Configure an MP-BGP neighbor.
	Configure MD5 authentication for BGP neighbors.
Configure BGP route generation.	Configure BGP to advertise local routes.
	Configuring BGP to redistribute routes.
	Configure BGP to advertise the default route.
Configure BGP route control.	Configure BGP to advertise aggregated routes.
	Configure the administrative distance of BGP routes.
	Configure routing policies in the outgoing direction of a BGP neighbor.
	Configure routing policies in the incoming direction of a BGP neighbor.
	Configure the maximum number of routes that a BGP neighbor receives.
	Configure the maximum number of BGP load balancing routes.

Configuration Tasks	
Configure BGP route properties.	Configure the BGP route weight.
	Configure the MED property of a BGP route.
	Configure the Local-Preference property of a BGP route.
	Configure the AS_PATH property of a BGP route.
	Configure the NEXT-HOP property of a BGP route.
	Configure the community property of a BGP route
Configure BGP network optimization.	Configure the keep-alive time of BGP neighbors.
	Configure BGP route detection time.
	Configure quick disconnection of EBGP neighbors.
	Configure the BGP route suppression function.
	Configure the BGP neighbor refresh capability.
	Configure the BGP neighbor soft reset capability.
	Configure the ORF capability of BGP neighbors.
Configure a large-scale BGP network.	Configure a BGP peer group.
	Configure a BGP route reflector.
	Configure a BGP confederation.
Configure BGP GR	Configure BGP GR Restarter
	Configure BGP GR Helper

Configuration Tasks	
Configure BGP to coordinate with BFD.	Configure EBGP to coordinate with BFD.
	Configure IBGP to coordinate with BFD.

6.13.2.1 Configure an IPv6 BGP Neighbor

Configuration Condition

Before configuring an IPv6 BGP neighbor, 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.

Configure an IBGP Neighbor

1. Perform basic configuration.

In configuring an IBGP neighbor, you need to set the AS of the neighbor to be the same as the AS of the local device. You can configure a Router ID for a device. The Router ID is used to uniquely identify a BGP device in setting up a BGP session. If no Router ID is configured for a device, the device selects a Router ID from interface addresses. The rules for selection are as follows:

- Select the biggest IP address from loopback interface IP addresses as the Router ID.
- If no loopback interface is configured with an IP address, select the biggest IP address from the IP addresses of other interfaces as the Router ID.
- Only when an interface is in the UP status can the IP address of the interface be elected as the Router ID.

Table 797 Configure an IBGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	Mandatory. By default, BGP is disabled.
Configure a Router ID for the BGP device.	bgp router-id *router-id*	Optional. By default, the device selects a Router ID from interface addresses. The loopback interface and large IP address have the priorities.
Configure an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	andatory. By default, no IBGP neighbor is created.
Configure a description for an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } description *description-string*	Optional. By default, no description is configured for an IBGP neighbor.
Enter the BGP IPv6 unicast configuration mode	address-family ipv6 unicast	-
Activate the capability of an IBGP neighbor in transmitting and receiving IPv6 unicast routes.	neighbor { *neighbor-address* | *peer-group-name* } activate	Optional. By default, the IBGP neighbor's capability in transmitting and receiving IPv6 unicast routes is not activated.

2. Configure the source address of a TCP session.

BGP uses the TCP protocol as the transport protocol. TCP features reliable transmission, ensuring that BGP protocol packets can be properly transmitted to its neighbors.

Table 798 Configure the source address of a TCP session

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no IBGP neighbor is created.
Configure the source address of a TCP session of an IBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } update-source { *interface-name* | *ipv6-address* }	Mandatory. By default, the TCP session automatically selects the address of a routing output interface as the source address.

Note

- If there are load balancing routes, the source addresses must be configured for TCP sessions of BGP neighbors. If TCP session source addresses are not configured, if the neighbors have different optimal routes, they may use different output interfaces as their source addresses. In this way, BGP sessions may fail to set up within a period of time.

Configure an EBGP Neighbor

1. Perform basic configuration.

In configuring an EBGP neighbor, you need to set the AS of the neighbor to be different from the AS of the local device.

Table 799 Configure an EBGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure an EBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no EBGP neighbor is created.

2. Configure a non-direct-connect EBGP neighbor

EBGP neighbors are located in different operation networks, and they are usually connected by a direct-connect physical link. Therefore, the default TTL value for the IP packets between EBGP neighbors is 1. In non-direct-connect operation networks, you can use a command to set the TTL value of IP packets so as to set up a BGP connection.

Table 800 Configure a non-direct-connect EBGP neighbor

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-

Step	Command	Description
Configure an EBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory. By default, no EBGP neighbor is created.
Configure the source address of a TCP session of an EBGP neighbor.	neighbor { *neighbor-address* | *peer-group-name* } update-source { *interface-name* | *ipv6-address* }	Optional. By default, the TCP session automatically selects the address of a routing output interface as the source address.
Allow non-direct-connect EBGP neighbors to set up a connection.	neighbor { *neighbor-address* | *peer-group-name* } ebgp-multihop [*ttl-value*]	Mandatory. By default, non-direct-connect devices are not allowed to form EBGP neighbors.

Configure a BGP Passive Neighbor

In some special application environments, the BGP passive neighbor function is in need. After the passive neighbor function is enabled, the BGP does not initiate the TCP connection request for setting up a BGP neighbor relation; instead, it waits for the neighbor's connection request before setting up a neighbor relation. By default, neighbors initiate connection requests to each other. If connections conflict, they select an optimal TCP connection to form a BGP session. Before configuring a BGP passive neighbor, you need to configure a BGP neighbor.

Table 801 Configure a BGP passive neighbor

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

Step	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*	Mandatory. By default, no BGP neighbor is created.
Configure a BGP passive neighbor.	neighbor { *neighbor-address* | *peer-group-name* } passive	Mandatory. By default, no passive neighbor is activated.

Configure an MP-BGP Neighbor

By default, the BGP neighbor can have the capability of receiving and sending the corresponding route when the VRF address family and VPN address family are activated. Before configuring an MP-BGP neighbor, you need to configure a BGP neighbor.

Table 802 Configure an MP-BGP neighbor

Step	Command	Description
Enter the 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*	Mandatory By default, do not create any BGP neighbor.
Enter the BGP IPv6 VRF configuration mode.	address-family ipv6 vrf *vrf-name*	-

Step	Command	Description
Configure the neighbors in the BGP IPv6 VRF address family	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory By default, do not create any BGP neighbor.
Activate the neighbors in IPv6 VRF address family.	neighbor { *neighbor-address* | *peer-group-name* } activate	Optional By default, the neighbors of the BGP IPv6 VRF configuration mode are activated.
Exit the BGP IPv6 VRF configuration mode.	exit-address-family	-

Note

- The neighbors that are configured in BGP configuration mode and BGP IPv6 unicast configuration mode are global neighbors, and the neighbors that are configured in BGP IPv6 VRF configuration mode belong only to the VRF address family.

Configure MD5 Authentication for BGP Neighbors

BGP supports configuring MD5 authentication to protect information exchange between neighbors. MD5 authentication is implemented by the TCP protocol. Two neighbors must be configured with the same authentication password before a TCP connection can be set up; otherwise, if the TCP protocol fails in MD5 authentication, the TCP connection cannot be set up. Before configuring MD5 authentication for BGP neighbors, you need to configure BGP neighbors.

Table 803 Configure MD5 authentication for BGP neighbors

Step	Command	Description
Enter the 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*	Mandatory. By default, no BGP neighbor is created.
Configure MD5 authentication for BGP neighbors.	neighbor { *neighbor-address* | *peer-group-name* } password [0 | 7] *password-string*	Mandatory. By default, no MD5 authentication is started for BGP neighbors.

6.13.2.2 Configure IPv6 BGP Route Generation

Configuration Condition

Before configuring IPv6 BGP route generation, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure BGP to Advertise Local Routes

BGP can use the **network** command to introduce the routes of the IPv6 route table into the BGP route table. Only when there are routes that match completely the **network** prefix and mask can the routes be introduced into the BGP route table and advertised.

In advertising a local route, you can apply a route map for the route, and you can also specify the route as the backdoor route. The backdoor route takes EBGP routes as

local BGP routes and uses the administrative distance of local routes. This allows IGP routes to have higher priorities than EBGP routes. At the same time, backdoor routes will not be advertised to EBGP neighbors.

Table 804 Configure BGP to advertise local routes

Step	Command	Description
Enter the 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 local routes.	network *ipv6-prefix* [route-map *rtmap-name* [backdoor] | backdoor]	Mandatory. By default, BGP does not advertise local routes.

Note

- The Origin property type of the local routes that are advertised by BGP is IGP.
- If you run the **network backdoor** command for an EBGP route, the administrative distance of the EBGP route changes to the local route administrative distance. (By default, the EBGP route administrative distance is 20, and the local route administrative distance is 200.), smaller than the default administrative distance of the IGP route, so that the IGP route is selected first, forming a backdoor link between EBGP neighbors.
- The route map applied to the local routes that are advertised by BGP supports match options, including as-path, community, extcommunity,

ipv6 address, ipv6 nexthop, and metric, and supports the set options, including as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

Configure BGP to Redistribute Routes

BGP is not responsible for route learning. It focuses mainly on managing route properties so as to control the route direction. Therefore, BGP redistributes IGP routes to generate BGP routes and advertise the BGP routes to neighbors. When BGP redistributes IGP routes, it can apply a routing diagram.

Table 805 Configure BGP to redistribute routes

Step	Command	Description
Enter the 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 redistribute IGP 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*]	Mandatory. By default, BGP does not redistribute IGP routes.

Note

- The Origin property type of the IGP routes that are advertised by BGP is INCOMPLETE.
- The route map applied to other protocol routes that are redistributed by BGP supports match options, including as-path, community, extcommunity, ipv6 address, ipv6 nexthop, and metric, and supports the set options, including as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

Configure BGP to Advertise the Default Route

Before BGP advertises a default route to neighbors, the default route needs to be introduced. Two ways of introducing the default routes are available: Running the **neighbor default-originate** command to generate a BGP default route, and running the **default-information originate** command to redistribute the default route of another protocol.

The default route that is generated by running the **neighbor default-originate** command is route ::/0 that is automatically generated by BGP. The default route that is redistributed by running the **default-information originate** command is route 0::/0 of the redistributed protocol introduced by BGP.

Table 806 Configure BGP to advertise the default route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enter the BGP IPv6 unicast	address-family ipv6 unicast	-

Step	Command	Description
configuration mode		
Configure BGP to generate the default route.	neighbor { *neighbor-address* | *peer-group-name* } default-originate [route-map *rtmap-name*]	Mandatory. By default, BGP does not generate the default route.
Configure BGP to re-distribute the default route of other protocols	default-information originate	Mandatory. By default, BGP does not redistribute the default route of another protocol.

Note

- In configuring BGP to redistribute the default route of another protocol, you need to configure BGP to redistribute routes.
- In configuring BGP to generate a default route, you can apply a route map to the route.
- The route map that is applied to the default route that is generated by BGP supports set options, including as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weigh.

6.13.2.3 Configure IPv6 BGP Route Control

Configuration Condition

Before configuring BGP route control, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure BGP to Advertise Aggregated Routes

In a large-scale BGP network, to decrease the number of routes that are advertised to neighbors or effectively control BGP routing, you can configure a BGP aggregated route.

Table 807 Configure BGP to advertise aggregated routes

Step	Command	Description
Enter the 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 aggregated routes.	aggregate-address *ipv6-prefix* [as-set / summary-only / route-map *rtmap-name*]	Mandatory. By default, BGP does not aggregate routes.

Note

- When configuring BGP to advertise aggregated routes, you can specify the **summary-only** option so that BGP advertises only aggregated routes. This decreases the number of routes that are advertised.
- You can specify the **as-set** option to generate aggregation routes with the AS_PATH property.
- You can also apply a route map to the aggregation routes so as to set more abundant properties for the aggregation routes.

Configure the Administrative Distance of BGP Routes

In the IP route table, each protocol controls the administrative distance of routing. The smaller the administrative distance is, the higher the priority is .BGP affects routing by specifying the administrative distances of specified network segments. The administrative distances of the routes that cover the specified network segments will be modified. Meanwhile, ACL is applied to filter the network segments that are covered by the routes, that is, only the administrative distances of the network segment that are allowed by the ACL can be modified.

The **distance bgp** command is used to modify the management distances of external, internal, and local BGP routes. The **distance** command is only used to modify the administrative distances of specified network segments. The **distance** command has a higher priority than the **distance bgp** command. The network segments that are covered by the **distance** command use the administrative distance that is specified by the command, while the network segments that are not covered by the distance command use the administrative distance that is specified by the **distance bgp** command.

Table 808 Configure the administrative distance of a BGP route

Step	Command	Description
Enter the 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 routes is 20, the administrative distance of
Configure the administrative distance of a specified network segment.	distance *administrative-distance ipv6-prefix* [*acl-num* | *acl-name*]	

Step	Command	Description
		IBGP routes is 200, and the administrative distance of local routes is 200.

Configure Routing Policies in the Outgoing Direction of a BGP Neighbor

BGP route advertising or routing is implemented based on the powerful routing properties. When advertising routes to neighbors, you can apply routing policies to modify route properties or filter some routes. Currently, the routing policies that can be applied in the outgoing direction include:

- distribute-list: Distribution list.
- filter-list: AS_PATH property filtration list.
- prefix-list: IP prefix list.
- route-map: Route map.

Table 809 Configure routing policies in the outgoing direction of a BGP neighbor

Step	Command	Description
Enter the 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	-
Apply the distribution list in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } distribute-list {*access-list-num* | *access-list-name* } out	You can select multiple options. (However, the distribution list and the IP prefix list cannot be configured at the same
Apply the AS_PATH property filtration list in the outgoing	neighbor { *neighbor-address* | *peer-group-name* } filter-list *aspath-list-*	

direction.	*name* out	time.) By default, no routing policy is configured in the outgoing direction of a BGP neighbor.
Apply the IP prefix list in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* out	
Apply a route map in the outgoing direction.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* out	

Note

- After configuring the routing policy in the outgoing direction of a BGP neighbor, you need to reset the neighbor to validate the settings.
- If you apply a route map in the outgoing direction of a route reflector, this changes only the NEXT-HOP property.
- For how to configure a filtration list, refer to the "Configure AS-PATH" section of the "Routing Policy Tools" chapter.
- In configuring routing policies in the outgoing direction of a BGP neighbor, you can configure multiple policies at the same time. BGP applies routing policies in the sequence of **distribute-list**, **filter-list**, **prefix-list**, and **route-map**. If a former policy is rejected, the latter policies will not be applied. The routing information can be advertised only after it passes all the configured policies.
- The route map that is applied in the outgoing direction of a BGP route supports match options, including as-path, community, extcommunity, ipv6 address, ip nexthop, and metric, and it supports the set options, including as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

Configure Routing Policies in the Incoming Direction of a BGP Neighbor

BGP can apply routing policies to filter received routing information or modify route properties. Similar to the policies applied in the outgoing directions, four polices are applied in the incoming directions:

distribute-list: Distribution list.

filter-list: AS_PATH property filtration list.

prefix-list: IPv6 prefix list.

route-map: Route map.

Table 810 Configure Routing Policies in the Incoming Direction of a BGP neighbor

Step	Command	Description
Enter the 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	-
Apply the distribution list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } distribute-list { *access-list-num* | *access-list-name* } in	You can select multiple options. (However, the distribution list and the IP prefix list cannot be configured at the same time.) By default, no policy is applied in the incoming direction.
Apply the AS_PATH property filtration list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } filter-list *aspath-list-name* in	
Apply the IP prefix list in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* in	
Apply a route map in the incoming direction.	neighbor { *neighbor-address* | *peer-group-name* } route-map	

Step	Command	Description
	rtmap-name in	

Note

- After configuring the routing policy in the incoming direction of a BGP neighbor, you need to reset the neighbor to validate the settings.
- In configuring routing policies in the incoming direction of a BGP neighbor, you can configure multiple policies at the same time. BGP applies routing policies in the sequence of **distribute-list**, **filter-list**, **prefix-list**, and **route-map**. If a former policy is rejected, the latter policies will not be applied. A route can be added into the database after it passes all the configured policies.
- The routing policies applied in the incoming direction of a BGP route support match options, including as-path, community, extcommunity, ipv6 address, ipv6 nexthop, and metric, and they support the set options, including as-path, comm-list, community, extcommunity, ipv6 next-hop, local-preference, metric, origin, and weight.

Configure the Maximum Number of Routes that a BGP Receives from a Neighbor

You can limit the number of routes that a BGP receives from a specified neighbor. Once the number of routes the BGP receives from the neighbor reaches a threshold, an alarm is generated or the neighbor is disconnected.

Table 811 Configure the maximum number of routes that a BGP Receives from a neighbor

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

Step	Command	Description
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 routes received by the neighbor.	neighbor { *neighbor-address* | *peer-group-name* } maximum-prefix *prefix-num* [*threshold-value*] [warning-only]	Mandatory. By default, the number of routes received by the neighbor.

Note

- If the **warning-only** option is not specified, after the number of routes that the BGP receives from the neighbor reaches the maximum number, the BGP session is automatically disconnected.
- If the warning-only option is specified, after the number of routes that the BGP receives from the neighbor reaches the maximum number, a warning message is displayed, but route learning continues.

Configure the Maximum Number of BGP Load Balancing Routes

In a BGP networking environment, if several paths with the same cost are available to reach the same destination, you can configure the number of BGP load balancing routes for load balancing.

Table 812 Configure the Maximum number of BGP load balancing routes

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

Step	Command	Description
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 IBGP load balancing routes.	maximum-paths ibgp *number*	Mandatory. By default, IBGP does not support load balancing routes.
Configure the maximum number of EBGP load balancing routes.	maximum-paths *number*	Mandatory. By default, EBGP does not support load balancing routes.

Note

- After the maximum number of EBGP load balancing routes is configured, load balancing takes effect only when EBGP routes are selected with priority.
- In different BGP configuration modes, the commands for configuring the maximum number of load balancing routes are different. For details, refer to the description of maximum-paths in the BGP technical manual.

6.13.2.4 Configure IPv6 BGP Route Properties

Configuration Condition

Before configuring BGP route properties, ensure that:

- BGP is enabled.

- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure the BGP Route Weight

In BGP routing, the first rule is to compare the weights of routes. The larger the weight of a route is, the higher the priority it has. The weight of a route is the local property of the device, and it cannot be transferred to other BGP neighbors. The value range of a route weight is 1-65535. By default, the weight of a route that has been learnt from a neighbor is 0, and the weights of all routes that are generated by the local device are all 32768.

Table 813 Configure the BGP route weight

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the weight of a route of a neighbor or peer group.	neighbor { *neighbor-address* | *peer-group-name* } weight *weight-num*	Mandatory. By default, the weight of a route of a neighbor is 0.

Configure the MED Property of a BGP Route

Multi-Exit Discriminator (MED) properties are used to select the optimal route for the traffic that enters an AS. If the other routing conditions are the same and BGP learns several routes with the same destination from different EBGP neighbors, BGP select the route with the minimum MED value as the optimal ingress.

MED sometimes is also called external metric. It is marked as a "metric" in the BGP route table. BGP advertises the MED properties of the routes that it has learnt from neighbors to IBGP neighbors, but BGP does not advertise the MED properties to EBGP neighbors. Therefore, MED properties are applicable to only adjacent ASs.

1. Configure BGP to allow comparing MEDs of neighbor routes from

different ASs.

By default, BGP implements MED route selection only among the routes that are from the same AS. However, you can run the **bgp always-compare-med** command to let BGP ignore the limitation on the same AS in MED route selection.

Table 814 Configure BGP to allow comparing MEDs of neighbor routes from different ASs

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to allow comparing MEDs of neighbor routes from different ASs.	bgp always-compare-med	Mandatory. By default, BGP allows only comparing MEDs of neighbor routes from the same AS.

2. Configure BGP to sort and select MEDs according to AS_PATH groups.

By default, BGP is not enabled to sort and select MEDs according to route AS_PATH groups. To enable the function, run the **bgp deterministic-med** command. In route selection, all routes are organized based on AS_PATHs. In each AS_PATH group, routes are sorted based on the MED values. The route with the minimum MED value is selected as the optimal route in the group.

Table 815 Configure BGP to sort and select MEDs according to AS_PATH groups

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration	router bgp *autonomous-system*	-

Step	Command	Description
mode.		
BGP sort and select MEDs according to AS_PATH groups	bgp deterministic-med	Mandatory By default, do not enable BGP to sort and select MEDs according to AS_PATH groups.

3. Configure to compare MEDs of routes in the local confederation.

By default, the MED values of EBGP routes from different ASs are not compared. The setting is valid for the EBGP routes of confederations. To enable comparison of MED values of routes of the local confederation, run the **bgp bestpath med confed** command.

Table 816 Configure BGP to compare MEDs of routes in the local confederation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to compare MED values of routes in the local confederation.	bgp bestpath med confed	Mandatory. By default, the MED values of routes in the local confederations will not be compared.

4. Configure a route map to modify MED properties.

In transmitting and receiving routes, you can apply a route map to modify MED

properties.

Table 817 Configure a route map to modify MED properties

Step	Command	Description
Enter the 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	-
Configuring a route map to modify MED properties.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an MED property, you can use the **set metric** command to modify the MED property. For details, refer to Routing Policy Tools-Technical Manual-**set metric**.
- After the **neighbor attribute-unchanged** command is configured, the MED properties of neighbors cannot be changed by the route map that is applied.

Configure the Local-Preference Property of a BGP Route

Local-Preference properties are transferred only between IBGP neighbors. Local-Preference is used to select the optimal egress of an AS. The route with the maximum Local-Preference will be selected with priority.

The value range of Local-Preference is 0-4294967295. The larger the value is, the higher priority the route has. By default, the Local-Preference value of all the routes that are advertised to IBGP neighbors is 100. You can use the **bgp default local-preference** command or the route map to modify the Local-Preference property value.

1. Configure BGP to modify the default Local-Preference property.

Table 818 Configure BGP to modify the default local-preference property

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure the default value of BGP Local-Preference property.	bgp default local-preference *local-value*	Optional. By default, the Local-Preference value is 100.

2. Configure the route map to modify the Local-Preference property.

Table 819 Configure the route map to modify the local-preference property

Step	Command	Description
Enter the 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 route map to modify the Local-Preference property.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, the route map is

Step	Command	Description
		not applied to any neighbor.

Note

- In configuring a route map to modify the Local-Preference property, you can use the **set local-preference** command to modify the Local-Preference property. For details, refer to Routing Policy Tools-Technical Manual-**set local-preference**.

Configure the AS_PATH Property of a BGP Route

1. Configure BGP to ignore AS_PATHs in route selection.

If the other conditions are the same, BGP selects the route with the shortest AS-PATH in route selection. To cancel route selection based on AS_PATHs, run the **bgp bestpath as-path ignore** command.

Table 820 Configure BGP to ignore AS_PATHs in route selection

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP to ignore AS_PATHs in route selection.	bgp bestpath as-path ignore	Mandatory. By default, the AS_PATH values are compared in route selection.

2. Configure the number of local ASs that BGP allows to repeat.

To prevent routing loops, BGP checks the AS_PATH properties of the routes that are received from neighbors, and the routes containing the local AS number will be discarded. However, you can run the **neighbor allowas-in** command to allow the AS_PATH properties of the routes that the BGP receives to contain the local AS number, and you can configure the number of ASs that can be contained.

Table 821 Configure the number of local ASs that BGP allows to repeat

Step	Command	Description
Enter the 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 ASs that are allowed to repeat.	neighbor { *neighbor-address* | *peer-group-name* } allowas-in [*as-num*]	Mandatory. By default, the AS_PATH properties of the routes that are received from neighbors do not allow the local AS number.

3. Configure BGP to remove the private AS number when advertising routes to neighbors.

In a large-scale BGP network, the AS_PATH properties of routes contain federation or community property. By default, BGP provides the private AS properties when it advertises routes to neighbors. To mask private network information, run the **neighbor remove-private-AS** command to remove the private AS number.

Table 822 Configure BGP to Remove the Private AS number when advertising routes to neighbors

Step	Command	Description
Enter the 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 remove the private AS number when advertising routes to neighbors.	neighbor { *neighbor-address* | *peer-group-name* } remove-private-AS	Mandatory. By default, when BGP advertise routes to neighbors, it provides the private AS number.

4. Configure to check the validity of the first AS number of an EBGP route.

When BGP advertises a route to EBGP neighbors, it compresses the local AS number to the starting position of the AS_PATH, and the AS that advertises the route first is located at the end. Usually, the first AS of a route that EBGP receives must be the same as the neighbor AS number; otherwise, the route will be discarded.

Table 823 Configure to check the validity of the first AS number of an EBGP route

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure to check the validity of the first AS number of an EBGP route.	bgp enforce-first-as	Mandatory. By default, BGP does not enable the mechanism for

Step	Command	Description
		checking the first AS number.

5. Configure a route map to modify AS_PATH properties.

BGP supports configuring a route map to modify AS_PATH properties. You can run the **set as-path prepend** command to add more routing properties so as to affect neighbor routing. In using the **set as-path prepend** function, first use the local AS to add AS_PATH. If you use another AS, the AS must be emphasized to prevent the AS from rejecting routes that are advertised to it.

Table 824 Configure a Route map to modify AS_PATH properties

Step	Command	Description
Enter the 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 AS_PATH properties.	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an AS_PATH property, you can use the **set as-path prepend** command to modify the AS_PATH property. For details, refer to Routing Policy Tools-Technical Manual-**set as-path**.

Configure the NEXT-HOP Property of a BGP Route

When BGP advertises routes to IBGP neighbors, it does not change the routing properties (including the NEXT-HOP property). When BGP advertises the routes that are learned from EBGP neighbors to IBGP neighbors, you can run the **neighbor next-hop-self** command to modify the next-hop property of the routes advertised to BGP neighbors to the local IP address. You can apply a route map to modify the next hop property.

1. Configure BGP to use the local IP address as the next hop of a route.

Table 825 Configure BGP to use the local IP address as the next hop of a route

Step	Command	Description
Enter the 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 use the local IP address as the next hop when advertising routes.	neighbor { *neighbor-address* | *peer-group-name* } next-hop-self	Mandatory. By default, the next-hop property of the routes that are advertised to EBGP neighbors is set to the local IPv6 address, and the next-hop property of the routes that are advertised to IBGP neighbors keeps unchanged.

Note

- When BGP is configured to use the local IPv6 address as the next hop of a route, if you run the **neighbor update-source** command to configure the source address of a TCP session, the source address is used as the next hop address; otherwise, the IP address of the output interface of the advertising device is selected as the local IPv6 address.

2. Configure a route map to modify NEXT-HOP properties.

BGP supports configuring a route map to modify NEXT-HOP properties. You can run the **set ipv6 next-hop** command to modify the next hop property.

Table 826 Configure a route map to modify NEXT-HOP properties

Step	Command	Description
Enter the 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 NEXT-HOP properties.	neighbor { neighbor-address | peer-group-name } route-map rtmap-name in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify an NEXT-HOP property, you can use

the **set ipv6 next-hop** command to modify the NEXT-HOP property. For details, refer to Routing Policy Tools-Technical Manual-**set ipv6 next-hop**.

Configure the Community Property of a BGP Route

When BGP advertises routes to neighbors, it can be configured to send the community property. You can apply a route map to a specified neighbor in the incoming and outgoing directions to match the community properties.

Community property is used to identify a group of routes so as to apply a routing policy to the group of routes. Two types of community property are available: standard and extended. The standard community property consist of 4 bytes, providing the properties such as NO_EXPORT, LOCAL_AS, NO_ADVERTISE, and INTERNET. The extended property consist of eight bytes, providing Route Target (RT) and Route Origin (RO) properties.

1. Configure BGP to advertise route community property to neighbors.

The **neighbor send-community** enables you to advertise standard community property or extended community property or both types of property to neighbors.

Table 827 Configure BGP to advertise route community property to neighbors

Step	Command	Description
Enter the 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 route community property to	neighbor { *neighbor-address* | *peer-group-name* } send-	Mandatory. By default, the community

neighbors.	community [both | extended | standard]	property is not advertised to any neighbor.

Note

- After neighbors are activated in VPNv6 address family, standard and extended community properties are automatically advertised to neighbors.

2. Configure a route map to modify the community property.

BGP supports configuring a route map to modify the route community property. You can use the **set communtiy** to command to modify the community property.

Table 828 Configure a route map to modify the community property

Step	Command	Description
Enter the 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 BGP route community property	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in | out	Mandatory. By default, no route map is applied to any neighbor.

Note

- In configuring a route map to modify community property, you can use the

set community command to modify the community property. For details, refer to Routing Policy Tools-Technical Manual-**set community**.

6.13.2.5 Configure IPv6 BGP Network Optimization

Configuration Condition

Before configuring BGP network optimization, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure the Keep-alive Time of BGP Neighbors

After a BGP session is successfully set up, keep-alive messages are sent periodically between the neighbors to maintain the BGP session. If no keep-alive message or Update packet is received from the neighbor within the hold time, the BGP session will be disconnected owing to timeout. The keep-alive time is equal to or smaller than 1/3 of the hold time.

Table 829 Configure the keep-alive time of BGP neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure global BGP keep-alive time and hold time.	timers bgp *keepalive-interval holdtime-interval*	Optional. By default, the keepalive timer is 60s, the hold timer is 180s, and the session re-connection timer is 120s.
Configure the keepalive time and hold time 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 hold time that are set for a specified neighbor have higher priorities than the global BGP keepalive time and hold time.
- Neighbors negotiate and then take the minimum hold time as the hold of the BGP session between the neighbors.
- If the keepalive time and hold time are both set to 0, the neighbor keepalive/hold function is canceled.
- If the keepalive time is longer than 1/3 of the hold time, the BGP session sends keepalive packets at the interval of 1/3 the hold time.

Configure BGP Route Detection Time

BGP mainly aims at implementing a routing process, with ASs as the routing units. Within an AS, IGP is used for routing. Therefore, BGP routes often rely on IGP routes. If the next hops or output interfaces of IGP routes that BGP relies on change, BGP detects IGP routes periodically to update BGP routes. BGP also update local BGP routes during the detection interval.

Table 830 Configure BGP route detection time

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure BGP route detection	bgp scan-time *time*	Optional.

time.		By default, the BGP route detection time is 60s.

Caution

- If the BGP route detection time is set too small, BGP detect routes frequently, affecting the device performance.

Configure Quick Disconnection of EBGP Neighbors

After a BGP session is successfully set up, Keepalive messages are sent periodically between the neighbors to maintain the BGP session. If no Keepalive message or Update packet is received from the neighbor within the hold time, the BGP session will be disconnected owing to timeout. You can configure direct-connect EBGP neighbors to disconnect a BGP connection immediately after a connecting interface is down, without waiting for BGP keepalive timeout. If the EBGP neighbor quick disconnection function is cancelled, the EBGP session does not respond to an interface down event; instead, the BGP session is disconnected after timeout.

Table 831 Configure quick disconnection of EBGP neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure quick disconnection of EBGP neighbors.	bgp fast-external-failover	Optional. By default, EBGP's quick processing capability in responding to the direct-connect interface down event is enabled.

Configure the BGP Route Suppression Function

Flapping routes in a network may cause instability of the network. You can configure route attenuation to damp this type of routes so as to decrease the effect of flapping routes on the network.

A frequently flapping route will be allocated with a penalty. If the penalty exceeds the suppression threshold, the route will not be advertised to neighbors. The penalty should not be kept beyond the maximum suppression time. If no flapping occurs on the route within the half-life period, the penalty will be halved. If the penalty is lower than the threshold value, the route can be advertised to neighbors again.

- Half-life period: It is the time in which the penalty of a route is halved.
- Reuse threshold: It is the threshold for the route to resume normal use.
- Suppression threshold: It is the threshold for route suppression.
- Maximum suppression time: It is the maximum time that the route is suppressed.

Table 832 Configure the BGP route suppression function

Step	Command	Description
Enter the 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 attenuation period.	bgp dampening [*reach-half-life* [*reuse-value suppress-value max-suppress-time* [*unreach-half-life*]] | route-map *rtmap-name*]	Mandatory. By default, the route suppression function is disabled. After the function is enabled, the default route

		suppression half-life period is 15 minutes, the route reuse time is 750, the route suppression threshold is 2000, the maximum route suppression time is 60 minutes, and the route penalty unreachable half-life period is 15 minutes.

Note

- Route flapping not only contains addition and deletion of routes, but also contains route property changes such as next hop and MED property changes.

Configure the BGP Neighbor Refresh Capability

If the routing policy or route selection policy that is applied to a BGP neighbor changes, the route table needs to be refreshed. One way of refreshing the route table is to reset the BGP connection so as to reset the BGP session. However, this mode may result in BGP route flapping, affecting normal services. The other way is more graceful, that is, configuring the local BGP device to support the route refresh capability. If a neighbor needs to reset a route, it advertises the Route-Refresh message to the local device. After receiving the Route-Refresh message, it sends the route to the neighbor again. In this way, the route table is dynamically refreshed without the need of disconnecting the BGP session.

Table 833 Configure the BGP Neighbor refresh capability

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enable the BGP neighbor refresh capability.	neighbor { *neighbor-address* | *peer-group-name* } capability route-refresh	Optional. By default, the BGP neighbor refresh capability is enabled.

Configure the BGP Neighbor Soft Reset Capability

If the routing policy or route selection policy that is applied to a BGP neighbor changes, the route table needs to be refreshed. One way of refreshing the route table is to reset the BGP connection so as to reset the BGP session. However, this mode may result in BGP route flapping, affecting normal services. Another way is more graceful, that is, configuring the local BGP device to support the route refresh capability. There is still another way, that is, enabling the soft reset capability of the local BGP device. By default, the BGP device reserves the routing information of each neighbor. After enabling its neighbor soft reset capability, it refreshes the neighbor routes that are kept on the local device. At this time, BGP sessions are not disconnected.

Table 834 Configure the BGP neighbor soft reset capability

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enter the BGP IPv6 unicast	address-family ipv6 unicast	-

Step	Command	Description
configuration mode		
Enable the BGP neighbor soft reset capability.	neighbor { *neighbor-address* | *peer-group-name* } soft-reconfiguration inbound	Mandatory. By default, the neighbor soft reset function is disabled.

Configure the ORF Capability of BGP Neighbors

BGP implements accurate route control through abundant routing properties. It usually applies routing policies in the incoming and outgoing directions. This mode is a local BGP behavior. BGP also supports the Outbound Route Filtering (ORF) capability. It advertises the local ingress policy to its neighbors through Route-refresh packets, and then the neighbors apply the policy when they advertise routes to the local BGP device. This greatly decreases the number of exchanged route refresh packets between BGP neighbors.

To achieve successful negotiation of the ORF capability, ensure that:

- The ORF capability is enabled for both neighbors.
- "ORF send" and "ORF receive" must match. That is, if one end is "ORF send", the other end must be "ORF both" or "ORF receive". If one end is "ORF receive", the other end must be "ORF send" or "ORF both".
- The "ORF send" end must be configured with a prefix list in the incoming direction.

Table 835 Configure the ORF capability of BGP neighbors

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-

Step	Command	Description
Enter the BGP IPv6 unicast configuration mode	address-family ipv6 unicast	-
Apply a prefix list in the incoming direction of a neighbor.	neighbor { *neighbor-address* | *peer-group-name* } prefix-list *prefix-list-name* in	Mandatory. By default, no prefix list is applied to any BGP neighbor.
Configure a neighbor to support the ORF capability.	neighbor { *neighbor-address* | *peer-group-name* } capability orf prefix-list { both | receive | send }	Mandatory. By default, a neighbor does not support the ORF capability.

6.13.2.6 Configure Large-Scale IPv6 BGP Network

Configuration Condition

Before configuring a large-scale BGP network, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure a BGP Peer Group

A BGP peer group is a group of BGP neighbors that are configured with the same configuration policy. Any configuration that is performed on a BGP peer group will take effect on all members of the peer group. In this way, by configuring the peer group, you can perform centralized management and maintenance on the neighbors.

Table 836 Configure a BGP peer group

Step	Command	Description
Enter the 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	Mandatory. By default, no peer group is configured, and a neighbor is not in any peer group.
Add a neighbor into the peer group.	neighbor *neighbor-address* peer-group *peer-group-name*	

Note

- The configuration on a peer group takes effect on all members of the peer group.
- After a neighbor is added into a peer group, if some configurations of the neighbor are the same as the configurations of the peer group, the configurations of the neighbor are deleted.
- If routing policies are configured in the incoming and outgoing directions of a peer group, after the routing policies are changed, the changes do not take effect on the neighbors that have been added into the peer group. To apply the changed routing policies on the peer group members, you need to reset the peer group.

Configure a BGP Route Reflector

In a large-scale BGP network, it is required that IBGP neighbors are fully connected, that is, each BGP needs to set up connections with all IBGP neighbors. In this way, in a network which contains N BGP neighbors, the number of BGP connections is N*(N-1)/2. The larger the number of connections is, the larger the number of route advertisements is. Configuring a BGP Route Reflector (RR) is a method of reducing the number of network connections. Multiple IBGPs are categorized into a group. In this group, a BGP is specified to act as the RR, while other BGPs act as client, and BGPs that are not in the group act as non-clients. Clients set up peer relations only with the RR while they do not set up peer relations with other BGPs. This reduces the number of mandatory IBGP connections, and the number of connections is N-1.

The following shoes the routing principles of the BGP RR:

- The RR reflects the routes that it learns from non-client IBGP neighbors only to clients.
- The RR reflects the routes that it learns from clients to all clients and non-clients except the clients that initiate the routes.
- The RR reflects the routes that it learns from EBGP neighbors to all clients and non-clients.

Table 837 Configure a BGP route reflector

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Configure an RR cluster ID.	bgp cluster-id { *cluster-id-in-ip* | *cluster-id-in-num* }	Mandatory. By default, the route ID is used as the RR cluster ID.

Step	Command	Description
Configure a neighbor as a client of the RR.	neighbor { *neighbor-address* | *peer-group-name* } route-reflector-client	Mandatory. By default, no neighbor is specified as a client of the RR.
Configure the route reflection function between BGP clients.	bgp client-to-client reflection	Optional. By default, the route reflection function is enabled between RR clients.

Note

- An RR cluster ID is used to identify an RR area. An RR area can contain multiple RRs, and the RRs in the RR area have the same RR cluster ID.

Configure a BGP Confederation

In a large-scale BGP network, it is required that IBGP neighbors are fully connected, that is, each BGP needs to set up connections with all IBGP neighbors. In this way, in a network which contains N BGP neighbors, the number of BGP connections is N*(N-1)/2. The larger the number of connections is, the larger the number of route advertisements is. Configuring BGP confederations is another way of reducing the number of network connections. An AS area is divided into multiple sub-AS areas, and each AS area forms a confederation. IBGP is adopted within a confederation to provide full connections, and sub-AS areas in the confederation are connected through EBGP connections. This effectively reduces the number of BGP connections.

In configuring BGP confederations, you need to assign a confederation ID for

each confederation and specify members for the confederation. In the case of route reflection, only the route reflector is required to support route reflection. However, in the case of a confederation, all members in a confederation must support the confederation function.

Table 838 Configure a BGP confederation

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Create a BGP confederation ID.	bgp confederation identifier *as-number*	Mandatory. By default, no AS number is configured for a confederation.
Configure members for the confederation.	bgp confederation peers *as-number-list*	Mandatory. By default, no sub-AS number is configured for a confederation.

Note

- A confederation ID is used to identify the sub-ASs of the confederation. Confederation members are divided into the sub-ASs.

6.13.2.7 Configure IPv6 BGP GR

Graceful Restart (GR) is used in active/standby switchover between devices. During the GR, the routing information of the local device and neighbor devices keep

unchanged at the forwarding layer, and data forwarding is not affected. After the switchover is completed and the new device starts to run, the two devices synchronize routing information at the protocol layer and update the forwarding layer so that data forwarding is not interrupted during the device switchover process.

Roles involved in a GR:

- GR Restarter: It is the device that is gracefully restarted.
- GR Helper: It is the device that helps with the GR.
- GR Time: It is the maximum time for GR-Restarters to restart. GR Helper maintains the stability of routes during the period of time.

A dual-controller device can act as a GR Restarter and a GR Helper, while a centralized device can only act as a GR Helper, helping the GR Restarter to complete a GR. When the GR Restarter is in the GR process, the GR Helper maintains the route stability until GR Time timeout. After the GR Helper helps with the GR, it synchronizes route information. During the process, network routes and packet forwarding keep the status before the GR, effectively ensuring the network stability.

The BGP GR relation is set up through OPEN packet negotiation when a connection is set up between neighbors. When the GR Restarter restarts the neighbor, the BGP session will be disconnected, but the routes that are learnt from the neighbor are not deleted. The routes are still normally forwarded in the IP route table. The routes are labeled with the Stale marks only in the BGP route table. After the GR is completed, the routes will be refreshed.

The GR Restarter needs to set up a connection with the GR Helper within the maximum allowed time (**restart-time**); otherwise, the GR Helper with cancel the maintained GR route and cancel the GR process. After the neighbor is re-connected, the GR Helper needs to receive an update packet with the End-Of-RIB mark from the GR Restarter to complete the GR process; otherwise, the GR route that is not updated will be deleted after the maximum hold time (**stalepath-time**) expires, and then the GR relation is released.

Configuration Condition

Before configuring a BGP GR, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure BGP GR Restarter

Table 839 Configure a BGP GR Restarter

Step	Command	Description
Enter the 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*]	Mandatory. By default, the GR capability is disabled for BGP devices. After the GR capability is enabled, the default maximum allowed time for re-setting up a session with the neighbor is 120s, and the maximum hold time of GR routes is 360s.
Enter the BGP IPv6 unicast configuration mode	address-family ipv6 unicast	-
Configure advertising the GR-Restarter capability to the neighbor	neighbor { *neighbor-address* | *peer-group-name* } capability graceful-restart	Mandatory By default, do not advertise the GR-Restarter capability

Step	Command	Description
		to the neighbor.

Configure BGP GR Helper

Table 840 Configure a BGP GR helper

Step	Command	Description
Enter the 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*]	Mandatory. By default, the GR capability is disabled for BGP devices. After the GR capability is enabled, the default maximum allowed time for re-setting up a session with the neighbor is 120s, and the maximum hold time of GR routes is 360s.

6.13.2.8 Configure IPv6 BGP to Coordinate with BFD

Usually, there are still some intermediate devices between BGP neighbors. When an intermediate device becomes faulty, the BGP session is normal within the hold time, and the link fault caused by the intermediate device cannot be responded to in time. Bidirectional Forwarding Detection (BFD) provides a method for quickly detecting the status of a line between two devices. After BFD is enabled for BGP devices, if a line between two devices becomes faulty, BFD can quickly find the line fault and notifies

BGP of the fault. It triggers BGP to quickly disconnect the session and quickly switch over to the backup line, achieving fast switchover of routes.

Configuration Condition

Before configuring BGP to coordinate with BFD, ensure that:

- BGP is enabled.
- IPv6 BGP neighbors are configured and a session is set up successfully.

Configure EBGP to Coordinate with BFD

The coordination between EBGP and BFD is based on a single-hop BFD session, and BFD session parameters need to be configured in interface mode.

Table 841 Configure EBGP to coordinate with BFD

Step	Command	Description
Enter the 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 coordinate with BFD.	neighbor { *neighbor-address* | *peer-group-name* } fall-over bfd [single-hop]	Mandatory. By default, the BFD function is disabled for a neighbor.
Exit the BGP IPv6 unicast configuration mode	exit-address-family	-
Exit the BGP configuration mode.	exit	-

Step	Command	Description
Enter the interface configuration mode.	interface *interface-name*	-
Configure the minimum receive interval of a BFD session.	bfd min-receive-interval *milliseconds*	Optional. By default, the minimum receive interval of a BFD session is 1000s.
Configure the minimum transmit interval of the BFD session.	bfd min-transmit-interval *milliseconds*	Optional. By default, the minimum transmit interval of a BFD session is 1000ms.
Configure the multiple of BFD session detection timeout.	bfd multiplier *number*	Optional. By default, the multiple of BFD session detection timeout is 5.

Note

- For the related configuration of BFD, refer to the reliability technology-BFD technical manual and BFD configuration manual.

Configure IBGP to Coordinate with BFD

The coordination between IBGP and BFD is based on a multi-hop BFD session, and BFD session parameters need to be configured in BGP mode.

Table 842 Configure IBGP to coordinate with BFD

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

Step	Command	Description
Enter the BGP configuration mode.	router bgp *autonomous-system*	-
Enter the BGP IPv6 unicast configuration mode	address-family ipv6 unicast	-
Configure IBGP to coordinate with BFD.	neighbor { *neighbor-address* | *peer-group-name* } fall-over bfd [single-hop]	Mandatory. By default, the BFD function is disabled for a neighbor.
Configure the minimum receive interval of the BFD session.	bfd min-receive-interval *milliseconds*	Optional. By default, the minimum receive interval of a BFD session is 1000s.
Configure the minimum transmit interval of the BFD session.	bfd min-transmit-interval *milliseconds*	Optional. By default, the minimum transmit interval of a BFD session is 1000ms.
Configure the multiple of BFD session detection timeout.	bfd multiplier *number*	Optional. By default, the multiple of BFD session detection timeout is 5.

6.13.2.9 Configure IPv6 BGP Fast Re-routing

Configuration Conditions

Before configuring IPv6 BGP fast re-routing, ensure that:

- When configuring fast rerouting based on route-map, the associated route-map has been configured.

- Enable the IPv6BG protocol.

Configure BGP Fast Re-routing

In the IPv6 BGP network, if the link or device fails, the packet passing the fault point will be dropped or generate the loop and the caused traffic interruption will not recover until the protocol re-converges, which often lasts for several seconds. To reduce the traffic interruption time, you can configure the IPv6 BGP fast re-routing. Apply the route map to set the backup next hop for the matched route. Once the active link fails, the traffic passing the faulty link will switch to the standby link at once, so as to realize fast switching.

Table 843 Configure the IPv6 BGP fast re-routing

Step	Command	Description
Enter the 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 fast re-routing based on route-map	fast-reroute route-map *route-map-name*	Mandatory By default, do not enable the fast re-routing function based on route-map.
Configure auto fast re-routing of BGP	pic	Mandatory By default, do not enable the auto fast re-routing function.

Caution

- After configuring the BGP fast re-routing, you need to re-set BGP and

complete the checking and backup of the initial route. Otherwise, it takes effect only for the route learned after configuration.

- For fast re-routing based on route-map, when configuring set fast-reroute backup-nexthop auto, the protocol performs auto fast re-routing.
- When using the pic mode, the protocol performs the auto fast re-routing.
- The various modes of enabling the fast re-routing are mutually exclusive.
- After configuring the BGP fast re-routing to apply the route map, set the BGP neighbor as the backup next hop via the **set fast-reroute backup-nexthop** *nexthop-address* command. If configuring the non-BGP neighbor as the backup next hop, you cannot make the fast re-routing function take effect.

6.13.2.10 IPv6 BGP Monitoring and Maintaining

Table 844 IPv6 BGP monitoring and maintaining

Command	Description
clear bgp ipv6 { * | *as-number* | peer-group *peer-group-name* | external | *neighbor-address* } [vrf *vrf-name*]	Resets the BGP neighbor.
clear bgp [ipv6 unicast] dampening [*ipv6-address* | *ipv6-address*/*mask-length*]	Clears suppressed routes.
clear bgp [ipv6 unicast] flap-statistics [*ipv6-address* | *ipv6-address*/*mask-length*]	Clears the flap statistics information
clear bgp [ipv6] { * | *as-number* | peer-group *peer-group-name* | external | *neighbor-address*} [vrf *vrf-name*] { [soft] [in | out] }	Soft-resets neighbors.
clear bgp [ipv6] { * | *neighbor-address* | *as-*	Advertises ORF to neighbors.

Command	Description
number | peer-group *peer-group-name* | external } [vrf *vrf-name*] in prefix-filter	
show bgp{ipv6 unicast | vpnv6 unicast vrf *vrf-name* } [*ipv6-address* | *ipv6-address/mask-length*]	Displays the routing information in the related BGP address family.
show ip bgp attribute-info	Displays the BGP common route attributes.
show bgp ipv6 unicast community [*community-number* / *aa:nn* / exact-match / local-AS / no-advertise / no-export]	Displays the routes that match the specified community property.
show bgp ipv6 unicast community-list *community-list-name*	Displays the community list that is applied to routes.
show bgp {ipv6 unicast | vpnv6 unicast vrf *vrf-name* } dampening { dampened-paths | flap-statistics | parameters }	Displays the details of route attenuation.
show bgp ipv6 unicast filter-list *filter-list-name* [exact-match]	Displays the routes that match the AS_PATH filter list.
show bgp ipv6 unicast inconsistent-as	Displays the routes that conflict with AS_PATH.
show bgp { ipv6 unicast | vpnv6 uicast vrf *vrf-name* } neighbors [*ipv6-address*]	Displays the details of the BGP neighbors
show bgp ipv6 unicast prefix-list *prefix-list-name*	Displays the routes that match the prefix list
show bgp ipv6 unicast quote-regexp *as-path-list-name*	Displays the routes that match the AS_PATH list
show bgp ipv6 unicast regexp *as-path-list-name*	Displays the routes that match the AS_PATH list

Command	Description
show bgp ipv6 unicast route-map *rtmap-name*	Displays the routes that match the route map
show ip bgp scan	Displays the BGP scan information.
show bgp {ipv6 unicast | vpnv6 vrf *vrf-name* } summary	Displays the summary of BGP neighbors.

6.13.3 IPv6 BGP Typical Configuration Example

6.13.3.1 Configure IPv6 BGP Basic Functions

Network Requirements

- Set up EBGP neighbors between Device1 and Device2, and set up IBGP neighbors between Device2 and Device3.
- Device1 learns the interface direct route 2001:4::/64 of Device3, and Device3 learns the interface direct route 2001:1::/64 of Device1.

Network Topology

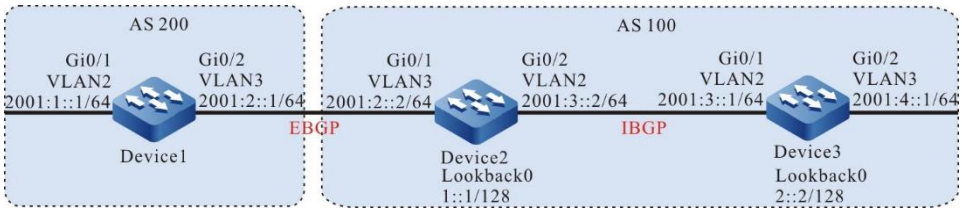


Figure 162 Networking for configuring IPv6 BGP basic functions

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that loopback routes are reachable between devices.

#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
```

#View the route 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:23:51:37, lo0
LC  1::1/128 [0/0]
     via ::, 00:09:34, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fec0:525a, 00:05:29, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:09:41, vlan3
```

```
L   2001:2::2/128 [0/0]
    via ::, 00:09:39, vlan3
C   2001:3::/64 [0/0]
    via ::, 00:08:55, vlan2
L   2001:3::2/128 [0/0]
    via ::, 00:08:53, vlan2
```

#View the route 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:18:34:53, lo0
O   1::1/128 [110/2]
    via fe80::201:7aff:fe5e:6d2e, 00:29:59, vlan2
LC  2::2/128 [0/0]
    via ::, 00:32:36, loopback0
C   2001:3::/64 [0/0]
    via ::, 00:32:59, vlan2
L   2001:3::1/128 [0/0]
    via ::, 00:32:58, vlan2
C   2001:4::/64 [0/0]
    via ::, 00:32:44, vlan3
L   2001:4::1/128 [0/0]
    via ::, 00:32:43, vlan3
```

According to the queried information, Device2 and Device3 have learnt the routes of the peer loopback interfaces by running OSPFv3, preparing for setting up IBGP neighbors on the loopback interfaces of Device2 and Device3.

Step 3: Configure the IPv6 BGP basic functions.

#Configure Device1.

Set up a direct-connect EBGP peer with Device2. Introduce 2001:1::/64 to BGP in network mode.

```
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.

Set up the direct-connect EBGP peer with Device1, set up a non-direct-connect IBGP peer with Device3 through Loopback0, and set the next hop of the advertised route to the local device.

```
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.

Set up a non-direct-connect IBGP peer relation with Device2 through Loopback0. Introduce 2001:4::/64 to BGP in network mode.

```
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 flapping, IBGP neighbors are set up through the loopback interfaces, and OSPFv3 need to synchronize the routing information of loopback interfaces between IBGP neighbors.

Step 4: Check the result.

#On Device2, check the IPv6 BGP neighbor status.

```
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
```

According to the numbers (Number of route prefixes received from neighbors) that are displayed in the State/PfxRcd column, IPv6 BGP neighbors have been successfully set up between Device 2 and Device 1, Device 3.

#View the route 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:00:42:57, lo0
C   2001:1::/64 [0/0]
     via ::, 00:02:59, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:02:56, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:52:17, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:52:16, vlan3
B   2001:4::/64 [20/0]
     via 2001:2::2, 00:06:13, vlan3
```

#View the route 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:00:34:53, lo0
LC  1::1/128 [0/0]
     via ::, 00:52:49, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fec0:525a, 00:48:45, vlan2
B   2001:1::/64 [20/0]
     via 2001:2::1, 00:03:18, vlan3
C   2001:2::/64 [0/0]
     via ::, 00:52:57, vlan3
L   2001:2::2/128 [0/0]
     via ::, 00:52:55, vlan3
C   2001:3::/64 [0/0]
     via ::, 00:52:10, vlan2
L   2001:3::2/128 [0/0]
     via ::, 00:52:09, lo0
B   2001:4::/64 [200/0]
     via 2::2, 00:07:27, vlan2
```

#View the route 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:18:54:38, lo0
O   1::1/128 [110/2]
     via fe80::201:7aff:fe5e:6d2e, 00:49:44, vlan2
LC  2::2/128 [0/0]
     via ::, 00:52:21, loopback0
B   2001:1::/64 [200/0]
     via 1::1, 00:03:54, vlan2
C   2001:3::/64 [0/0]
     via ::, 00:52:44, vlan2
L   2001:3::1/128 [0/0]
     via ::, 00:52:43, vlan2
C   2001:4::/64 [0/0]
     via ::, 00:52:29, vlan3
L   2001:4::1/128 [0/0]
     via ::, 00:52:28, vlan3
```

Device1 has learnt the interface direct-connect route 2001:4::/64 of Device3, and Device3 has learnt the interface direct-connect route 2001:1::/64 of Device1.

6.13.3.2 Configure IPv6 BGP to Re-distribute Routes

Network Requirements

- Set up OSPFv3 neighbors between Device3 and Device2, and advertise interface direct-connect route 2001:3::/64 to Device2.
- Set up EBGP neighbors between Device1 and Device2, and redistribute the OSPFv3 route that Device2 learns to BGP and advertise the route to Device1.

Network Topology

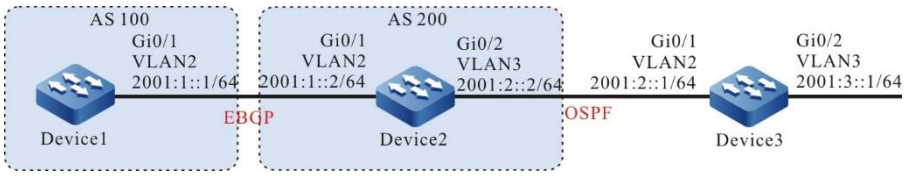


Figure 163 Networking for configuring IPv6 BGP to redistribute routes

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that Device2 can learn the direct-connect interface route 2001:3::/64 to 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
```

#View the route 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:01:10:38, lo0
C   2001:1::/64 [0/0]
    via ::, 00:06:25, vlan2
L   2001:1::2/128 [0/0]
    via ::, 00:06:24, vlan2
C   2001:2::/64 [0/0]
    via ::, 00:05:46, vlan3
L   2001:2::2/128 [0/0]
    via ::, 00:05:43, vlan3
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fec0:525a, 00:02:41, vlan3
```

According to the route table, Device2 has learnt the OSPFv3 route 2001:3::/64 that has been advertised by Device3.

Step 3: Configure the IPv6 BGP basic functions.

#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
```

#On Device2, check the IPv6 BGP neighbor status.

```
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
```

IPv6 BGP neighbors have been successfully set up between Device2 and Device1.

Step 4: Configure IPv6 BGP to redistribute the OSPFv3 route.

#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.

#View the IPv6 BGP route 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
```

```
[0]*> 2001:2::/64       ::                  1          32768 ?
[0]*> 2001:3::/64       ::                  2          32768 ?
```

According to the queried information, OSPFv3 routes have been successfully redistributed to IPv6 BGP.

#View the route 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 ?
```

According to the queried information, Device1 has successfully learnt routes 2001:2::/64 and 2001:3::/64.

Note

- In an actual application, if there are two or more AS boundary routers, it is recommended that you do not redistribute routes between different routing protocols. If route redistribution must be configured, you are required to configure route control policies such as route filtering and filtration summary on the AS boundary routers to prevent routing loops.

6.13.3.3 Configure IPv6 BGP Community Properties

Network Requirements

- Set up EBGP neighbors between Device1 and Device2.
- Device1 introduces two direct-connect routes 2001:1::/64 and 2001:2::/64 to BGP in network mode, and set different community properties for two routes that are advertised to Device2.

- When Device2 receives routes from Device1, it applies community properties in the incoming direction of a neighbor to filter route 2001:1::/64 and allow route 2001:2::/64.

Network Topology

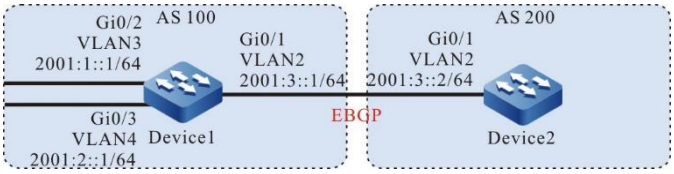


Figure 164 Networking for configuring IPv6 BGP community properties

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure the IPv6 BGP basic functions.

#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
```

#On Device1, check the IPv6 BGP neighbor status.

```
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 00:01:02        0

Total number of neighbors 1
```

IPv6 BGP neighbors have been successfully set up between Device1 and Device2.

#Query the route 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:05:45:34, lo0
B    2001:1::/64 [20/0]
     via 2001:3::1, 00:01:35, vlan2
B    2001:2::/64 [20/0]
     via 2001:3::1, 00:01:35, vlan2
C    2001:3::/64 [0/0]
     via ::, 00:04:09, vlan2
L    2001:3::2/128 [0/0]
     via ::, 00:04:08, vlan2
```

According to the queried information, Device2 has successfully learnt routes 2001:1: :/64 and 2001:2::/64.

Step 3: Configure the ACL and routing policy, and set IPv6 BGP community properties.

#Configure Device1.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:1::/64 any
Device1(config-v6-list)#commit
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)#commit
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 properties for routes 2001:1::/64 and 2001:2::/64 respectively by configuring an ACL and routing policy.

Step 4: Configure a routing 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
```

#View the IPv6 BGP route 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: 00:00:24 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: 00:00:30 ago
```

According to the IPv6 BGP route table of Device2, the community property of route 2001:1::/64 is set to 100:1, and the community properties of route 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.

#View the route 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:05:58:57, lo0
B   2001:2::/64 [20/0]
     via 2001:3::1, 00:00:05, vlan2
C   2001:3::/64 [0/0]
     via ::, 00:17:32, vlan2
L   2001:3::2/128 [0/0]
     via ::, 00:17:30, vlan2
```

According to the IPv6 BGP route table of Device2, route 2001:1::/64 has been

filtered in the incoming direction, and route 2001:2::/64 has been allowed.

Note

- After a routing policy is configured on the IPv6 BGP neighbor, the IPv6 BGP must be reset to make the configuration take effect.
- You must configure the **send-community** command to advertise the community property to the peer.

6.13.3.4 Configure IPv6 BGP Route Reflector

Network Requirements

- Set up EBGP neighbors between Device3 and Device4, and configure Device4 to advertise route 2001:4::/64.
- Set up IBGP neighbors between Device2 and Device3 and between Device2 and Device1 respectively. On Device2, configure Route Reflectors (RRs), and configure Device1 and Device3 as clients, so that Device1 can learn route 2001:4::/64 that is advertised by Device4.

Network Topology

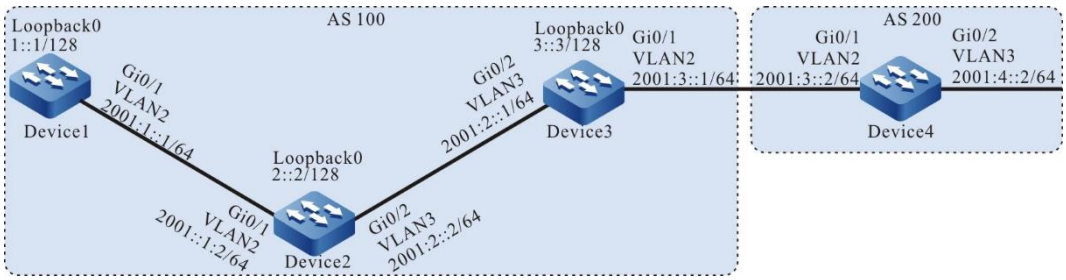


Figure 165 Networking for configuring an IPv6 BGP route reflector

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that loopback routes are reachable between devices.

#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
```

#View the route 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:06:26:16, lo0
LC  1::1/128 [0/0]
     via ::, 00:13:56, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fec0:525a, 00:09:06, vlan2
O   3::3/128 [110/3]
     via fe80::201:7aff:fec0:525a, 00:00:36, vlan2
C   2001:1::/64 [0/0]
     via ::, 00:14:03, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:14:02, vlan2
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec0:525a, 00:09:06, vlan2
```

#View the route 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:00:46:09, lo0
O   1::1/128 [110/2]
     via fe80::201:7aff:fe5e:6d2e, 00:10:05, vlan2
LC  2::2/128 [0/0]
     via ::, 00:14:23, loopback0
O   3::3/128 [110/2]
     via fe80::201:7aff:fe62:bb80, 00:01:44, vlan3
C   2001:1::/64 [0/0]
     via ::, 00:14:48, vlan2
L   2001:1::2/128 [0/0]
     via ::, 00:14:47, vlan2
```

```
C   2001:2::/64 [0/0]
    via ::, 00:14:41, vlan3
L   2001:2::2/128 [0/0]
    via ::, 00:14:39, vlan3
```

#View the route 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:06:37:24, lo0
O   1::1/128 [110/3]
    via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
O   2::2/128 [110/2]
    via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
LC  3::3/128 [0/0]
    via ::, 00:14:45, loopback0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
C   2001:2::/64 [0/0]
    via ::, 00:15:03, vlan3
L   2001:2::1/128 [0/0]
    via ::, 00:15:02, vlan3
C   2001:3::/64 [0/0]
    via ::, 00:14:55, vlan2
L   2001:3::1/128 [0/0]
    via ::, 00:14:54, vlan2
```

According to the route table, Device1, Device2, and Device3 have learnt the routes of the loopback interfaces of each other.

Step 3: Configure the IPv6 BGP basic functions.

#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
```

#On Device2, check the IPv6 BGP neighbor status.

```
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
```

#On Device4, check the IPv6 BGP neighbor status.

```
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 00:01:45        0

Total number of neighbors 1
```

According to the queried information, IPv6 BGP neighbors have been set up between the devices.

#Query the IPv6 BGP route 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
```

#View the IPv6 BGP route 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 route table of Device1.

```
Device1#show bgp ipv6 unicast
```

According to the above result, Device2 and Device3 have learnt route 2001:4::/64, and Device2 has not advertised the route to Device1.

Step 4: Configure an 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, Device1 and Device3 have been configured as the RR clients.

Step 5: Check the result.

#View the route 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:06:48:52, lo0
LC  1::1/128 [0/0]
     via ::, 00:36:32, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
O   3::3/128 [110/3]
     via fe80::201:7aff:fec0:525a, 00:23:12, vlan2
C   2001:1::/64 [0/0]
     via ::, 00:36:39, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:36:38, vlan2
O   2001:2::/64 [110/2]
     via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
B   2001:4::/64 [200/0]
     via 3::3, 00:01:16, vlan2
```

On BGP of Device2, Device1 and Device3 have been configured as the RR clients, and Device2 has successfully reflects route 2001:4::/64 to RR client Device1.

Note

- If you configure an IPv6 BGP neighbor as a RR client, the neighbor will be reset.

6.13.3.5 Configure IPv6 BGP Route Summary

Network Requirements

- Set up OSPFv3 neighbors between Device1 and Device3, and configure Device3 to advertise routes 2002:1::/64 and 2002:2::/64 to Device1.
- Set up EBGP neighbors between Device1 and Device2.
- On Device1, aggregate routes 2002:1::/64 and 2002:2::/64 into route 2002::/30 and advertise the aggregated route to Device2.

Network Topology

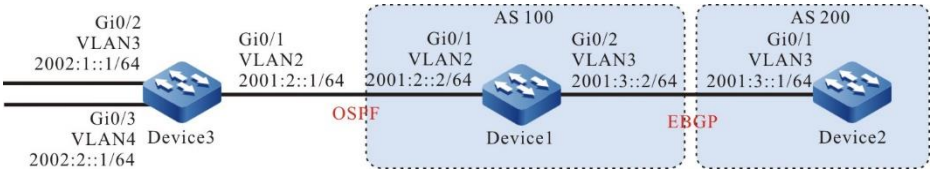


Figure 166 Networking for configuring IPv6 BGP route summary

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that Device1 can learn the 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
```

#View the route 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:07:35:38, lo0
C   2001:3::/64 [0/0]
     via ::, 00:01:11, vlan3
L   2001:3::2/128 [0/0]
     via ::, 00:01:10, vlan3
C   2001:2::/64 [0/0]
     via ::, 00:01:06, vlan2
L   2001:2::2/128 [0/0]
     via ::, 00:01:04, vlan2
O   2002:1::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2
O   2002:2::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2
```

According to the route table, Device1 has learnt routes 2002:1:1::/64 and 2002:1:2::/64 advertised by Device3.

Step 3: Configure the IPv6 BGP basic functions.

#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)# exit-address-family
Device2(config-bgp)#exit
```

#On Device1, check the IPv6 BGP neighbor status.

```
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 00:01:16        0
```

IPv6 BGP neighbors have been successfully set up between Device1 and Device2.

Step 4: Configure IPv6 BGP route summary.

Two solutions are available to complete the network requirements.

Solution 1: Configure an IPv6 static route that is targeted at null0 to introduce the the static route 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.

#View the IPv6 BGP route 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
```

You can see that the aggregated route 2002::/30 is generated in the IPv6 BGP route table of Device1.

#View the route 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:03:14:01, lo0
C   2001:3::/64 [0/0]
     via ::, 01:20:21, vlan3
L   2001:3::1/128 [0/0]
     via ::, 01:20:20, vlan3
B   2002::/30 [20/0]
     via 2001:3::2, 00:00:44, vlan3
```

Device2 has successfully learnt the aggregated route 2002::/30 that has been advertised by Device1.

Solution 2: First introduce detailed routes into BGP, and then run the **aggregate-address** command to aggregate the routes.

#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 route 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
[0]*> 2001:2::/64       ::                   1          32768 ?
[B]*> 2002::/30         ::                              32768 i
[0]s> 2002:1::/64       ::                   2          32768 ?
[0]s> 2002:2::/64        ::                  2          32768 ?
```

The aggregated route 2002::/30 has been generated in the IPv6 BGP route table of Device1.

#View the route 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:03:16:42, lo0
B   2001:2::/64 [20/0]
    via 2001:3::2, 00:00:50, vlan3
C   2001:3::/64 [0/0]
    via ::, 01:23:01, vlan3
L   2001:3::1/128 [0/0]
    via ::, 01:23:00, vlan3
B   2002::/30 [20/0]
    via 2001:3::2, 00:00:50, vlan3
```

Device2 has successfully learnt the aggregated route 2002::/30 that has been advertised by Device1.

Note

- When the **aggregate-address** command is used to aggregate routes, if the extended command **summary-only** is configured, the device advertises only the aggregated route; otherwise, both common routes and aggregated routes are advertised.

6.13.3.6 Configure the IPv6 BGP Route Selection Priority

Network Requirements

- 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.
- Device1 advertises two routes 2001:1::/64 and 2001:2::/64 to Device4, and Device4 advertises two routes 2001:7::/64 and 2001:8::/64 to Device1.
- Modify the Local-preference property of routes on Device2 and Device3 so that Device1 selects route 2001:7::/64 advertised by Device2 and route 2001:8::/64 advertised by Device3 with priority.

- Modify the MED property of routes on Device2 and Device3 so that Device4 selects route 2001:1::/64 advertised by Device3 and route 2001:2::/64 advertised by Device2 with priority.

Network Topology

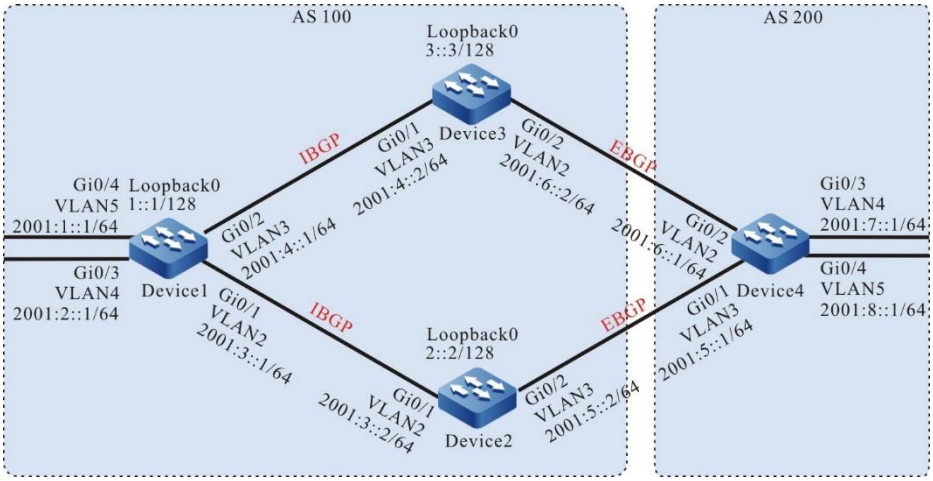


Figure 167 Networking for configuring the IPv6 BGP route selection priority

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that loopback routes are reachable between devices.

#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
```

#View the route 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:04:03:11, lo0
LC  1::1/128 [0/0]
    via ::, 00:08:39, loopback0
O   2::2/128 [110/2]
    via fe80::201:7aff:fe5e:87da, 00:02:04, vlan2
O   3::3/128 [110/2]
    via fe80::201:7aff:fec0:525b, 00:00:38, vlan3
C   2001:1::/64 [0/0]
    via ::, 00:09:12, vlan5
L   2001:1::1/128 [0/0]
```

```
    via ::, 00:09:11, vlan5
C   2001:2::/64 [0/0]
    via ::, 00:08:26, vlan4
L   2001:2::1/128 [0/0]
    via ::, 00:08:26, vlan4
C   2001:3::/64 [0/0]
    via ::, 00:09:01, vlan2
L   2001:3::1/128 [0/0]
    via ::, 00:09:00, vlan2
C   2001:4::/64 [0/0]
    via ::, 00:08:55, vlan3
L   2001:4::1/128 [0/0]
    via ::, 00:08:53, vlan3
```

#View the route 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:23:16:51, lo0
O   1::1/128 [110/2]
    via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
LC  2::2/128 [0/0]
    via ::, 00:09:31, loopback0
O   3::3/128 [110/3]
    via fe80::201:7aff:fe62:bb7f, 00:02:52, vlan2
C   2001:3::/64 [0/0]
    via ::, 00:09:49, vlan2
L   2001:3::2/128 [0/0]
    via ::, 00:09:48, vlan2
O   2001:4::/64 [110/2]
    via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
C   2001:5::/64 [0/0]
    via ::, 00:09:39, vlan3
L   2001:5::2/128 [0/0]
    via ::, 00:09:38, vlan3
```

#View the route 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:22:16:55, lo0
O   1::1/128 [110/2]
    via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
O   2::2/128 [110/3]
    via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
LC  3::3/128 [0/0]
    via ::, 00:10:48, loopback0
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
C   2001:4::/64 [0/0]
    via ::, 00:11:55, vlan3
L   2001:4::2/128 [0/0]
    via ::, 00:11:54, vlan3
C   2001:6::/64 [0/0]
    via ::, 00:11:48, vlan2
L   2001:6::2/128 [0/0]
    via ::, 00:11:47, vlan2
```

According to the route table, Device1, Device2, and Device3 have learnt the routes of the loopback interfaces of each other.

Step 3: Configure the IPv6 BGP basic functions.

#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
```

#On Device1, check the IPv6 BGP neighbor status.

```
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
```

#On Device4, check the IPv6 BGP neighbor status.

```
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 00:02:43        2
2001:6::2       4   100       5       6        4    0    0 00:02:32        2

Total number of neighbors 2
```

IBGP neighbors have been set up between Device1 and Device2 and between Device2 and Device3, and EBGP neighbors have been set up between Device4 and Device2 and between Device4 and Device3.

#View the route 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:04:20:19, lo0
LC  1::1/128 [0/0]
     via ::, 00:25:47, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fe5e:87da, 00:19:12, vlan2
O   3::3/128 [110/2]
     via fe80::201:7aff:fec0:525b, 00:17:46, vlan3
C   2001:1::/64 [0/0]
     via ::, 00:26:20, vlan5
L   2001:1::1/128 [0/0]
     via ::, 00:26:19, vlan5
C   2001:2::/64 [0/0]
```

```
    via ::, 00:25:34, vlan4
L   2001:2::1/128 [0/0]
    via ::, 00:25:34, vlan4
C   2001:3::/64 [0/0]
    via ::, 00:26:09, vlan2
L   2001:3::1/128 [0/0]
    via ::, 00:26:08, vlan2
C   2001:4::/64 [0/0]
    via ::, 00:26:03, vlan3
L   2001:4::1/128 [0/0]
    via ::, 00:26:01, vlan3
B   2001:7::/64 [200/0]
    via 2::2, 00:03:21, vlan2
B   2001:8::/64 [200/0]
    via 2::2, 00:02:57, vlan2
```

According to the route table, both route 2001:7::/64 and route 2001:8::/64 of Device1 select Device2 as the next-hop device.

#Query the route 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:04:14:15, lo0
B   2001:1::/64 [20/0]
    via 2001:5::2, 00:06:52, vlan2
B   2001:2::/64 [20/0]
    via 2001:5::2, 00:06:52, vlan2
```

```
C   2001:5::/64 [0/0]
    via ::, 00:26:17, vlan3
L   2001:5::1/128 [0/0]
    via ::, 00:26:16, vlan3
C   2001:6::/64 [0/0]
    via ::, 00:26:24, vlan2
L   2001:6::1/128 [0/0]
    via ::, 00:26:23, vlan2
C   2001:7::/64 [0/0]
    via ::, 00:25:53, vlan4
L   2001:7::1/128 [0/0]
    via ::, 00:25:51, vlan4
C   2001:8::/64 [0/0]
    via ::, 00:25:40, vlan5
L   2001:8::1/128 [0/0]
    via ::, 00:25:40, vlan5
```

Both route 2001:1::/64 and 2001:2::/64 of Device4 select Device3 as the next-hop device.

Step 4: Configure an ACL and routing policy to 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)#commit
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)#commit
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
```

On Device2, configure a routing policy to set local-preference of route 2001:8::/64 to 110, and set metric of 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)#commit
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)#commit
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
```

On Device3, configure a routing policy to set local-preference of route 2001:7::/64 to 110, and set metric of route 2001:2::/64 to 100.

Note

- In configuring a routing 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 a routing 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
```

On Device2, configure the outgoing direction of neighbor 1::1 to modify local-preference of route 2001:8::/64, and configure the outgoing direction of neighbor 2001:5::1 to modify metric of route 2001:1::/64.

#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
```

On Device3, configure the outgoing direction of neighbor 10.0.0.1 to modify local-preference of route 2001:7::/64, and configure the outgoing direction of neighbor 2001:6::1 to modify metric of route2001:2::/64.

After a routing policy is configured on the neighbor, you need to reset the neighbor.

Step 6: Check the result.

#View the route 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:04:59:59, lo0
LC  1::1/128 [0/0]
     via ::, 01:05:27, loopback0
O   2::2/128 [110/2]
     via fe80::201:7aff:fe5e:87da, 00:58:52, vlan2
O   3::3/128 [110/2]
     via fe80::201:7aff:fec0:525b, 00:57:26, vlan3
C   2001:1::/64 [0/0]
     via ::, 01:06:00, vlan5
L   2001:1::1/128 [0/0]
     via ::, 01:05:59, vlan5
C   2001:2::/64 [0/0]
     via ::, 01:05:14, vlan4
L   2001:2::1/128 [0/0]
     via ::, 01:05:14, vlan4
C   2001:3::/64 [0/0]
     via ::, 01:05:49, vlan2
L   2001:3::1/128 [0/0]
     via ::, 01:05:48, vlan2
C   2001:4::/64 [0/0]
     via ::, 01:05:43, vlan3
L   2001:4::1/128 [0/0]
     via ::, 01:05:41, vlan3
B   2001:7::/64 [200/0]
     via 3::3, 00:09:05, vlan3
B   2001:8::/64 [200/0]
     via 2::2, 00:04:58, vlan2
```

According to the route table, local-preference of routes 2001:7::/64 and 2001:8::/64 is modified successfully, and Device1 select route 2001:8::/64 that is advertised by Device2 and route2001:7::/64 that is advertised by Device3 with priority.

#Query the route 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:04:53:45, lo0
B   2001:1::/64 [20/0]
     via 2001:6::2, 00:12:10, vlan3
B   2001:2::/64 [20/0]
     via 2001:5::2, 00:07:40, vlan2
C   2001:5::/64 [0/0]
     via ::, 01:05:47, vlan3
L   2001:5::1/128 [0/0]
     via ::, 01:05:46, vlan3
C   2001:6::/64 [0/0]
     via ::, 01:05:54, vlan2
L   2001:6::1/128 [0/0]
     via ::, 01:05:52, vlan2
C   2001:7::/64 [0/0]
     via ::, 01:05:22, vlan4
L   2001:7::1/128 [0/0]
     via ::, 01:05:21, vlan4
C   2001:8::/64 [0/0]
     via ::, 01:05:09, vlan5
L   2001:8::1/128 [0/0]
     via ::, 01:05:09, vlan5
```

According to the route table, metric of routes 2001:1::/64 and 2001:2::/64 is modified successfully, and Device4 select route 2001:2::/64 that is advertised by

Device2 and route 2001:1::/64 that is advertised by Device3 with priority.

Note

- A routing policy can be used in the outgoing direction of route advertisement, and it can also be used in the incoming direction of route receiving.

6.13.3.7 Configure IPv6 BGP to Coordinate with BFD

Network Requirements

- Set up EBGP neighbors between Device1 and Device2 and between Device1 and Device3, and set up IBGP neighbors between Device2 and Device3.
- Device1 learns EBGP route 2001:3::/64 both from Device2 and Device3, and Device1 selects to forward data to the network segment 2001:3::/64 through Device2.
- On Device1 and Device2, configure EBGP to coordinate with BFD. When the line between Device1 and Device2 becomes faulty, BFD can quickly detect the fault and notify BGP of the fault. Then Device1 selects to forward data to network segment 2001:3::/64 through Device3.

Network Topology

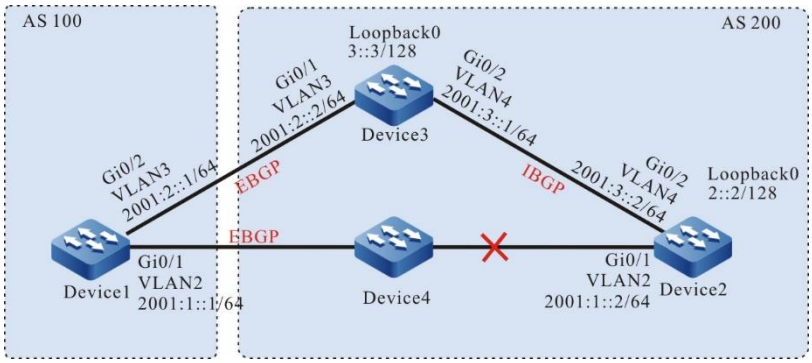


Figure 168 Networking for configuring IPv6 BGP to coordinate with BFD

Configuration Steps

Step 1: Configure the IPv6 global unicast addresses of the interfaces. (Omitted)

Step 2: Configure OSPFv3 so that loopback routes are reachable between devices.

#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
```

#View the route 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:09:31:22, lo0
LC  2::2/128 [0/0]
     via ::, 00:10:10, loopback0
O   3::3/128 [110/1]
     via fe80::201:7aff:fec0:525a, 00:00:12, vlan4
C   2001:1::/64 [0/0]
     via ::, 00:10:54, vlan2
L   2001:1::2/128 [0/0]
     via ::, 00:10:53, vlan2
C   2001:3::/64 [0/0]
     via ::, 00:10:17, vlan4
L   2001:3::2/128 [0/0]
     via ::, 00:10:16, vlan4
```

#View the route 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:03:50:38, lo0
O   2::2/128 [110/2]
     via fe80::201:7aff:fe5e:6d2e, 00:02:40, vlan4
LC  3::3/128 [0/0]
     via ::, 00:00:49, loopback0
C   2001:2::/64 [0/0]
     via ::, 00:03:03, vlan3
L   2001:2::2/128 [0/0]
     via ::, 00:03:02, vlan3
C   2001:3::/64 [0/0]
     via ::, 00:03:18, vlan4
L   2001:3::1/128 [0/0]
     via ::, 00:03:17, vlan4
```

According to the route table, Device2 and Device3 have learnt the routes of the loopback interfaces of each other.

Step 3: Configure an ACL and routing policy to set the metric of a route.

#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)#commit
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
```

The routing policy that is configured on Device1 sets the metric of route 2001:3::/64 to 50.

Step 4: Configure the IPv6 BGP basic functions, and associate Device1 the routing policy.

#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
```

After a routing policy is configured on the peer, you need to reset the peer.

#On Device1, check the IPv6 BGP neighbor status.

```
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 00:04:00        1
2001:2::2       4   200       5       5        2    0    0 00:02:03        1

Total number of neighbors 2
```

#On Device2, check the IPv6 BGP neighbor status.

```
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 00:02:10        1
2001:1::1       4   100       6       7        2    0    0 00:04:38        0

Total number of neighbors 2
```

IPv6 BGP neighbors between Device1, Device2, and Device3 have been set up successfully.

```
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:09:53:27, lo0
C   2001:1::/64 [0/0]
     via ::, 00:24:05, vlan2
L   2001:1::1/128 [0/0]
     via ::, 00:24:02, vlan2
C   2001:2::/64 [0/0]
     via ::, 00:25:21, vlan3
L   2001:2::1/128 [0/0]
     via ::, 00:25:20, vlan3
B   2001:3::/64 [20/0]
     via 2001:1::2, 00:05:06, vlan2
```

According to the route table, route 2001:3::/64 of Device1 selects Device2 as the 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
```

BFD is enabled between EBGP neighbors Device1 and Device2, and the minimum transmit interval, minimum receive interval, and detection timeout multiple of the BFD control packets have been modified.

Step 6: Check the result.

#On Device1, query the BFD session status.

```
Device1#show bfd session ipv6
OurAddr                    NeighAddr                  State     Holddown   Interface
2001:1::1                  2001:1::2                  UP        2000       vlan2
```

On Device1, the BFD status is up, and the holddown time is negotiated to be 2000ms.

#If the line between Device1 and Device2 becomes faulty, the route can quickly switch over to the backup line.

#View the route 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, lo0
C   2001:1::/64 [0/0]
```

```
    via ::, 00:37:08, vlan2
L   2001:1::1/128 [0/0]
    via ::, 00:37:04, vlan2
C   2001:2::/64 [0/0]
    via ::, 00:38:24, vlan3
L   2001:2::1/128 [0/0]
    via ::, 00:38:23, vlan3
B   2001:3::/64 [20/0]
    via 2001:2::2, 00:00:16, vlan3
```

The next hop of route 2001:3::/64 is Device3.

6.13.3.8 Configure IPv6 BGP Static Fast Re-routing

Network Requirements

- All devices are configured with the IPv6 BGP protocol.
- Enable the static fast rerouting between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

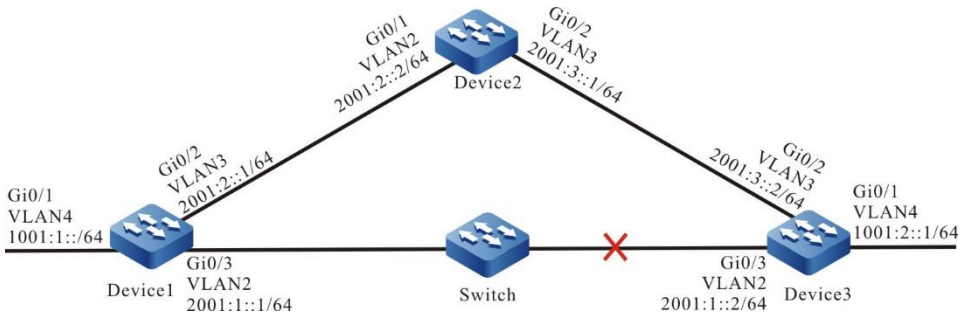


Figure 169 Networking of configuring IPv6 BGP static fast re-routing

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IPv6 address of the interface (omitted).

Step 2: Configure BGP.

#Configure Device1 to set up the BGP neighbor with Device2 and Device3.

```
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 300
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2 to set up the BGP neighbor with Device1 and Device3.

```
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 2001:2::1 remote-as 100
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 300
Device2(config-bgp-af)#exit-address-family
Device2 (config-bgp)#exit
```

#Configure Device3 to set up the BGP neighbor with Device1 and Device2.

```
Device3(config)#router bgp 300
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6 unicast
Device3(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device3(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device3(config-bgp-af)#network 1001:2::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next-hop interface vlan3, and the next-hop address 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_bgp
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set ipv6 fast-reroute backup-interface vlan3 backup-nexthop
2001:2::2
Device1(config-route-map)#exit
```

Step 4: Configure the static fast re-routing.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6 unicast
Device1(config-bgp-af)#fast-reroute route-map ipv6frr_bgp
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

Step 5: Check the result.

#View the IPv6 BGP route 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 ::, 23:12:10, lo0
C   1001:1::/64 [0/0]
    via ::, 23:07:17, vlan4
L   1001:1::1/128 [0/0]
    via ::, 23:07:17, vlan4
B   1001:2::/64 [20/0]
    via 2001:1::2, 00:03:25, vlan2
C   2001:1::/64 [0/0]
    via ::, 13:47:06, vlan2
L   2001:1::1/128 [0/0]
    via ::, 13:47:06, vlan2
C   2001:2::/64 [0/0]
    via ::, 23:06:35, vlan3
L   2001:2::1/128 [0/0]
    via ::, 23:06:35, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 FRR table of Device1.

```
Device1#show ipv6 frr 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
B   1001:2::/64 [20/4294967295]
    via 2001:2::2, 00:05:16, vlan3
```

You can see that the next-hop of the frr route is 2001:2::2, and the outgoing

interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6  2001:1::1 detail
Total ipv6 session number: 1
OurAddr          NeighAddr         LD/RD              State     Holddown    Interface
2001:1::1        2001:1::1         1016/1016          UP        500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:73  Remote Discriminator:73
Local State:UP  Remote State:UP  Up for: 0h:8m:52s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is set up normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 23:18:47, lo0
C   1001:1::/64 [0/0]
     via ::, 23:13:54, vlan4
L   1001:1::1/128 [0/0]
     via ::, 23:13:54, vlan4
B   1001:2::/64 [20/0]
     via 2001:2::2, 00:00:03, vlan3
C   2001:2::/64 [0/0]
     via ::, 23:13:12, vlan3
L   2001:2::1/128 [0/0]
     via ::, 23:13:12, vlan3
```

6.13.3.9 Configure IPv6 BGP Dynamic Fast Re-routing

Network Requirements

- All devices are configured with the IPv6 BGP protocol.
- Enable the dynamic fast rerouting between Device1 and Device3. When the line fails, the service can be quickly switched to Device2 for communication.

Network Topology

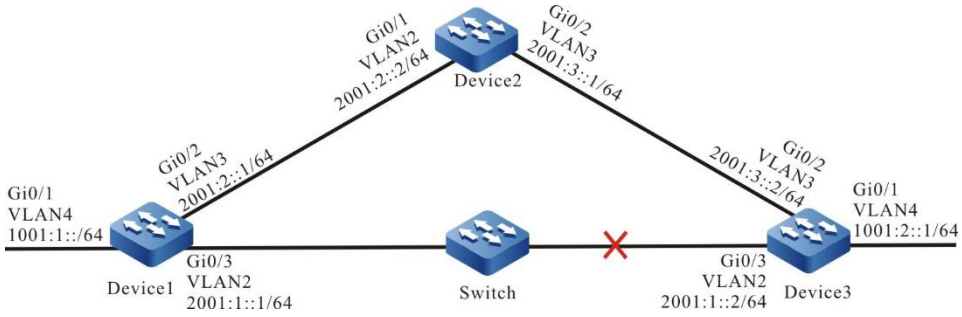


Figure 170Networking of configuring the IPv6 BGP dynamic fast re-routing

Configuration Steps

Step 1: Configure VLAN, and add the port to the corresponding VLAN; configure the IPv6 address of the interface (omitted).

Step 2: Configure BGP.

#Configure Device1 to set up the BGP neighbor with Device2 and Device3.

```
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 300
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#Configure Device2 to set up the BGP neighbor with Device1 and Device3.

```
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 2001:2::1 remote-as 100
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 300
Device2(config-bgp-af)#exit-address-family
```

```
Device2 (config-bgp)#exit
```

#Configure Device3 to set up the BGP neighbor with Device1 and Device2.

```
Device3(config)#router bgp 300
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6 unicast
Device3(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device3(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device3(config-bgp-af)#network 1001:2::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

Step 3: Configure the routing policy.

#Configure Device1, configure route-map, and call ACL to match only 1001:2::1/64, while other network segments will be filtered out. The routing application matching the match rule backs up the next-hop interface vlan3, and the next-hop address 2001:2::2.

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 1001:2::1/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map ipv6frr_bgp
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)# set ipv6 fast-reroute backup-nexthop auto
Device1(config-route-map)#exit
```

Step 5: Configure the static fast re-routing.

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6 unicast
Device1(config-bgp-af)#fast-reroute route-map ipv6frr_bgp
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

Step 5: Check the result.

#View the IPv6 BGP route 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 ::, 23:12:10, lo0
C   1001:1::/64 [0/0]
    via ::, 23:07:17, vlan4
L   1001:1::1/128 [0/0]
    via ::, 23:07:17, vlan4
B   1001:2::/64 [20/0]
    via 2001:1::2, 00:03:25, vlan2
C   2001:1::/64 [0/0]
    via ::, 13:47:06, vlan2
L   2001:1::1/128 [0/0]
    via ::, 13:47:06, vlan2
C   2001:2::/64 [0/0]
    via ::, 23:06:35, vlan3
L   2001:2::1/128 [0/0]
    via ::, 23:06:35, vlan3
```

It can be seen from the routing table that route 1001:2::/64 preferably communicates with the line between Device1 and Device3.

#View the IPv6 FRR table of Device1.

```
Device1#show ipv6 frr 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
B   1001:2::/64 [20/4294967295]
    via 2001:2::2, 00:05:16, vlan3
```

You can see that the next-hop of the frr route is 2001:2::2, and the outgoing interface is vlan3.

#View the BFD session information of Device1.

```
Device1#show bfd session ipv6  2001:1::1 detail
Total ipv6 session number: 1
OurAddr          NeighAddr        LD/RD            State     Holddown    Interface
2001:1::1        2001:1::1        1032/1032        UP        500         vlan2
Type:ipv6 direct  Mode:echo
Local Discriminator:73  Remote Discriminator:73
Local State:UP  Remote State:UP  Up for: 0h:8m:52s  Number of times UP:1
Send Interval:100ms  Detection time:500ms(100ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
Registered modules:FIB_MGR
```

You can see that FIB_MGR is linked with BFD successfully, the session is set up normally, and the session mode is echo.

#After the line between Device1 and Device3 fails, it can quickly detect and switch to Device2 for communication. Check the routing table of Device1. In the routing table, the outgoing interface to the destination network 1001:2::/64 has been switched to the backup interface vlan3.

```
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 ::, 23:18:47, lo0
C   1001:1::/64 [0/0]
     via ::, 23:13:54, vlan4
L   1001:1::1/128 [0/0]
     via ::, 23:13:54, vlan4
B   1001:2::/64 [20/0]
     via 2001:2::2, 00:00:03, vlan3
C   2001:2::/64 [0/0]
     via ::, 23:13:12, vlan3
L   2001:2::1/128 [0/0]
     via ::, 23:13:12, vlan3
```

6.14 PBR

6.14.1 Overview

The PBR (policy-based routing) is a routing mechanism for forwarding the packets based on the user-defined policy. When the packet is forwarded in the route, the packet can be matched based on the ACL rule, such as the IP protocol number, source IP address, destination address, and the length. For the packets that match the matching rules, destination IP address, source TCP/UDP port number, destination TCP/UDP number, packet priority, and TCP identifier. For the packets satisfying the matching rule, perform the operation according to the specified policy. (set the next hop for the packet) In this way, forwarding control of the packets is implemented.

Traditional routing forwards packets only based on the destination addresses. Compared with the traditional routing, the PBR is more flexible. It is an effective supplement to and enhancement of the traditional routing mechanism.

6.14.2 PBR Function Configuration

Table 845 PBR configuration list

Configuration Task	
Configure the PBR	Configure the next hop IP address for forwarding the packet
	Configure the standby next hop IP address for forwarding the packet
	Configure the next-hop IPv6 address of the packet forwarding
	Configure the standby next-hop IPv6 address of the packet forwarding
	Configure the PBR action group to bind with the ACL
	Configure the PBR action group to bind with the ACL rule
Configure the PBR application	Configure to apply the ACL with PBR to the L2/L3 Ethernet interface
	Configure to apply the ACL with PBR to the VLAN
	Configure to apply the ACL with PBR to Interface VLAN
	Configure to apply the ACL with PBR to the vlan range
	Configure to apply the ACL with PBR to the interface vlan range
	Configure to apply the ACL with PBR globally
	Configure to apply the ACL with PBR to VXLAN

Configuration Task	
	Configure to apply the ACL with PBR to Interface VXLAN

6.14.2.1 Configure PBR

The PBR is achieved depending on the packet filtering by the ACL rule. The ACL rule first filters the qualified packets and then forward the packets to the next hop by executing the PBR.

Configuration Condition

Before configuring the PBR function, first complete the following task:

- Configure the ACL and the ACL rule.

Configure Next Hop IP Address for Forwarding Packet

Configure the next hop IP address for the forwarding the packet to specify the destination IP address of the PBR.

Up to 6 next hop IP addresses can be specified for forwarding the packet. If the user configures multiple next hop IP addresses simultaneously and multiple next hop IP addresses are reachable, then the packet will choose the next hop IP address for forwarding using the load balancing mode.

Table 846 Configure the next hop IP address for forwarding the packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the PBR action group configuration mode	pbr-action-group *pbr-action-group-name*	-
Configure the next hop IP	redirect ipv4-nexthop *ip-*	Mandatory

Step	Command	Description
address for forwarding the packet	*address*[track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [vrf *vrf-name*]	By default, the next hop IP address for forwarding the packet is not configured.

Note

- If all the configured next hop IP addresses are unreachable, then the PBR function will not take effect.
- The next hop IP address cannot be configured as the multicast IP address and broadcast IP address.
- PBR supports being associated with TRACK ID, realizing the linkage with TRACK status.

Configure Standby Next Hop IP Address for Forwarding Packet

Configure the standby next hop IP address for the forwarding the packet to specify the destination IP address of the PBR.

When the active next hop is not reachable, if the standby next hop IP address is reachable, the packet will be forwarded to the standby next hop IP address. If the active next hop is reachable, the packet will continue to be forwarded to the active next hop IP address.

Up to four standby next hops can be configured and the priorities are reduced in turn. The standby next hops take effect in priority order. If the primary next hop is unreachable and the IP address of the first standby next hop is reachable, the packet

will be forwarded to the IP address of the first standby next hop; If the first standby next hop IP address is unreachable and the second standby next hop IP address is reachable, the packet will be forwarded to the second standby next hop IP address. And so on.

Table 847 Configure the standby next hop IP address for forwarding the packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the PBR action group configuration mode	pbr-action-group *pbr-action-group-name*	-
Configure the standby next hop IP address for forwarding the packet	redirect ipv4-nexthop backup *ip-address*[track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [*ip-address*] [track *track-id*] [vrf *vrf-name*]	Mandatory By default, the standby next hop IP address for forwarding the packet is not configured.

Note

- If all the configured standby next hop IP addresses are unreachable, then the PBR function will not take effect.
- The next hop IP address cannot be configured as the multicast IP address and broadcast IP address.
- PBR supports being associated with TRACK ID, realizing the linkage with TRACK status.

Configure the Next-hop IPv6 Address of Packet Forwarding

Configure the next-hop IPv6 address of the packet forwarding, so as to specify the destination address of the policy route.

You can specify six next-hop IPv6 addresses of the packet forwarding at most. If the user configures multiple next-hop IPv6 addresses at the same time, and there are multiple next-hop IPv6 addresses reachable, the packet adopts the load balancing mode to specify the next-hop IPv6 address for forwarding.

Table 848 Configure the next-hop IPv6 address of the packet forwarding

Step	Command	Description
Enter the 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 of the packet forwarding	redirect ipv6-nexthop *ipv6-address* [track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*] [vrf *vrf-name*]	Mandatory By default, do not configure the next-hop IPv6 address of the packet forwarding.

Note

- If the configured next-hop IPv6 addresses are unreachable, then the PBR function will not take effect.
- The next-hop IP address cannot be configured as the local IPv6 address, multicast address, or broadcast address.
- PBR supports being associated with TRACK ID, realizing the linkage with

TRACK status.

Configure Standby Next Hop IPv6 Address for Forwarding Packet

Configure the standby next hop IPv6 address for the forwarding the packet to specify the destination IP address of the PBR.

When the active next hop is not reachable, if the standby next hop IPv6 address is reachable, the packet will be forwarded to the standby next hop IPv6 address. If the active next hop is reachable, the packet will continue to be forwarded to the active next hop IPv6 address.

Up to four standby next hops can be configured and the priorities are reduced in turn. The standby next hops take effect in priority order. If the primary next hop is unreachable and the IPv6 address of the first standby next hop is reachable, the packet will be forwarded to the IPv6 address of the first standby next hop; If the first standby next hop IPv6 address is unreachable and the second standby next hop IPv6 address is reachable, the packet will be forwarded to the second standby next hop IPv6 address. And so on.

Table 849 Configure the standby next hop IPv6 address for forwarding the packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the PBR action group configuration mode	pbr-action-group *pbr-action-group-name*	-
Configure the standby next hop IPv6 address for forwarding the packet	redirect ipv6-nexthop backup *ipv6-address*[track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*] [*ipv6-address*] [track *track-id*]	Mandatory By default, the standby next hop IPv6 address for forwarding the packet is not

Step	Command	Description
	[vrf *vrf-name*]	configured.

Note

- If the configured standby next hop IPv6 addresses are unreachable, then the PBR function will not take effect.
- The next hop IPv6 address cannot be configured as the multicast IP address and broadcast IP address.
- PBR supports being associated with TRACK ID, realizing the linkage with TRACK status.

Configure PBR Action Group to Bind with ACL

Configure the PBR action group to bind with the ACL to achieve all rules in the ACL to associate with the PBR execution actions.

After the PBR action group is bound to the ACL, all rules in the ACL will establish the association with the PBR execution actions. If the packet received by the interface matches the ACL rule, then the packet will be forwarded to the next hop.

Table 850 Configure the PBR action group to bind with the ACL

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the PBR action group to bind with the ACL	ip pbr-action-group *pbr-action-group-name* access-list { *access-list-number* | *access-list-name* }	Optional By default, the PBR action group is not bound with the IP ACL.

Step	Command	Description
		The PBR action group supports the IP ACL binding. The IP ACL contains the 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, do not bind PBR action group with the IPv6 ACL. The PBR action group supports IPv6 ACL binding. IPv6 ACL contains IPv6 standard ACL and IPv6 extended ACL.

Note

- Only when the configured next hop IP address is reachable, the PBR can take effect.
- The PBR can take effect only for the rules allowed in the ACL.

Configure PBR Action Group to Bind ACL Rule

Configure the PBR action group to bind with the ACL rule to achieve the ACL rule to associate with the PBR execution actions.

After the PBR action group is bound to the ACL rule, the ACL rule will establish the association with the PBR execution actions. If the packet received by the interface matches the ACL rule, then the packet will be forwarded to the next hop specified by

the action group.

Table 851Configure the PBR action group to bind with the ACL rule

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the PBR action group to bind with the ACL rule	Refer to the section "Configure IP standard ACL". Refer to the section "Configure IP extended ACL". Refer to “Configure IPv6 Standard ACL”. Refer to “Configure IPv6 Extended ACL”.	In the permit rules of the IP standard ACL and extended ACL, the PBR action group must be specified to take the PBR into effect. When configuring the permit rules of the IPv6 standard ACL and extended ACL, the PBR action group must be specified to take the PBR into effect.

Note

- Only when the configured next hop IP address is reachable, the PBR can take effect.
- The PBR can take effect only for the rules allowed in the ACL.

6.14.2.2 Configure PBR Application

The PBR application actually is the application of the ACL with the PBR. The validation of the PBR depends on the ACL rule. The ACL can be applied to the L2/L3 Ethernet interface, VLAN, Interface VLAN, VXLAN, Interface VXLAN, VLAN RANGE, Interface VLAN RANGE, and globally.

When the ACL with the PBR is applied to L2/L3 Ethernet interface, VLAN, Interface VLAN and globally, it may cause collision. In this case, the PBR corresponding to the high priority takes effect and the priority in the descending order is as follows: port, VLAN/Interface VLAN, VLAN RANGE/Interface VLAN RANGE, and global.

Configuration Condition

None

Configure to Apply ACL with PBR to L2/L3 Ethernet Interface

After the ACL with the PBR is applied to the L2/L3 Ethernet interface, the corresponding L2/L3 Ethernet interface will have the PBR function.

Table 852 Configure to apply the PBR to the L2/L3 Ethernet interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 Ethernet interface configuration mode, the subsequent configuration can only take effect on the current interface. After entering the aggregation group configuration mode, t the subsequent configuration can only take effect on the aggregation group.
Enter the aggregation group configuration mode	link-aggregation *link-aggregation-id*	
Configure to apply the PBR to the interface	ip policy-based-route { *access-list-number* | *access-*	Optional By default, the interface

Step	Command	Description
	list-name }	does not apply the IP ACL with PBR.
	ipv6 policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, the interface does not apply the IPv6 ACL with PBR.

Configure to Apply ACL with PBR to VLAN

After the ACL with PBR is applied to the VLAN, all interfaces in the corresponding VLAN will have the PBR function.

Table 853 Configure to apply the PBR to the VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	-
Apply the PBR to the VLAN	ip policy-based-route{access-*list-number* | *access-list-name* }	Optional By default, the VLAN does not apply the IP ACL with PBR.

Configure to Apply ACL with PBR to Interface VLAN

After the ACL with PBR is applied to the Interface VLAN, the corresponding Jnterface VLAN interfaces will have the PBR function.

Table 854 Configure to apply the PBR to Interface VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Interface VLAN configuration mode	Interface vlan *vlan-id*	-
Configure to apply the PBR to Interface VLAN	ip policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, Interface VLAN is not applied to the IP ACL with the PBR.
	ipv6 policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, Interface VLAN is not applied to the IPv6 ACL with the PBR.

Configure to Apply ACL with PBR to VLAN RANGE

After the ACL with PBR is applied to VLAN RANGE, the corresponding VLAN RANGE will have the PBR function.

Table 855 Configure to apply the PBR to VLAN RANGE

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure to apply the PBR to VLAN RANGE	ip policy-based-route { *access-list-number* | *access-list-name* } vlan range <1-4094>	Optional By default, the IP ACL with the PBR is not applied to VLAN RANGE.

Step	Command	Description
	ipv6 policy-based-route { *access-list-number* | *access-list-name* } vlan range <1-4094>	Optional By default, the IPv6 ACL with the PBR is not applied to VLAN RANGE.

Configure to Apply ACL with PBR to Interface VLAN RANGE

After the ACL with PBR is applied to Interface VLAN RANGE, the corresponding VLAN RANGE will have the PBR function.

Table 856 Configure to apply the PBR to Interface VLAN RANGE

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure to apply the PBR to VLAN RANGE	ip policy-based-route { *access-list-number* | *access-list-name* } interface vlan range <1-4094>	Optional By default, the IP ACL with the PBR is not applied to Interface VLAN RANGE.
	ipv6 policy-based-route { *access-list-number* | *access-list-name* }interface vlan range <1-4094>	Optional By default, the IPv6 ACL with the PBR is not applied to Interface VLAN RANGE.

Configure to Apply ACL with PBR Globally

After the ACL with PBR is applied globally, all interfaces on the device will have the PBR function.

Table 857 Configure to apply the PBR globally

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure to apply the PBR globally	global ip policy-based-route { *access-list-number* | *access-list-name* }	Mandatory By default, the ACL with PBR is not applied globally.

Configure to Apply ACL with PBR to VXLAN

After the ACL with PBR is applied to a VXLAN, the VXLAN will have the PBR function.

Table 858 Configure to apply the PBR to VXLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	-
Configure to apply the PBR to VXLAN	ip policy-based-route{ *access-list-number* | *access-list-name* }	Optional By default, the IP ACL with PBR is not applied to the VXLAN.

Configure to Apply ACL with PBR to Interface VXLAN

After the ACL with PBR is applied to an Interface VXLAN, the Interface VXLAN will have the PBR function.

Table 859 Configure to apply the PBR to Interface VXLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Interface VXLAN configuration mode	Interface vxlan *vxlan-id*	-
Configure to apply the PBR to Interface VXLAN	ip policy-based-route { *access-list-number* | *access-list-name* }	Optional By default, the IP ACL with PBR is not applied to Interface VXLAN.

6.14.2.3 PBR Monitoring and Maintaining

Table 860 PBR monitoring and maintaining

Command	Description
show pbr-action-group [*pbr-action-group-name*]	Display the PBR configuration information.
show policy-based-route object [global | interface [vlan | switchport | routedport | vlan-range] | vlan | vlan-range | vxlan-vnid | vxlan-l3vnid]	Display the PBR configuration information. If not specifying the parameter, display all PBR application information.

6.14.3 PBR Typical Configuration Example

6.14.3.1 Configure PBR

Network Requirement

- Device1 has the default route and the gateway is Device2.
- Configure the PBR on Device1 to enable PC to visit the network 1.1.1.0/24 via Device3 and visit network 1.1.2.0/24 via Device2.

Network Topology

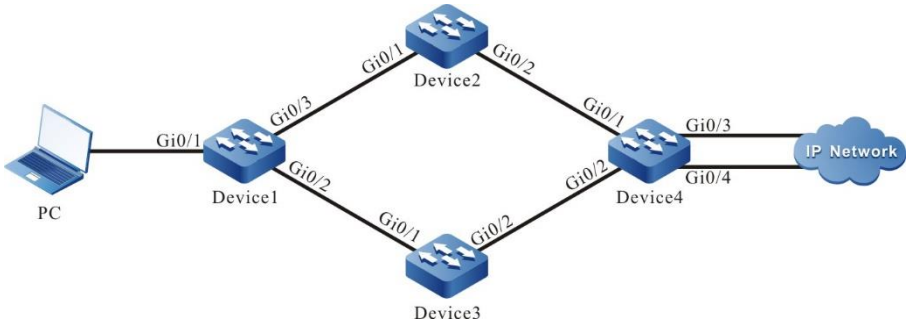


Figure 171 Networking of configuring the PBR

Device	Interface	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 the VLAN and join the interface to the corresponding VLAN. (Omitted)

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure the 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
```

#View 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, 00:00:59, vlan2
C   20.1.1.0/24 is directly connected, 00:00:50, vlan3
C   30.1.1.0/24 is directly connected, 00:00:39, vlan4
C   127.0.0.0/8 is directly connected, 03:47:36, lo0
```

Step 4: Configure the PBR on Device1.

#Configure the PBR action group and redirect the packet to the 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)#exit
```

#View the PBR action group information on Device1.

```
Device1#show pbr-action-group pbr
pbr-action-group pbr
redirect ipv4-nexthop 20.1.1.2(valid)
```

#Configure the ACL and bind the ACL rule matching the destination IP network segment 1.1.1.0/24 with the 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)#commit
Device1(config-std-nacl)#exit
```

#View 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 l3-action-group pbr (active)
 20 permit ip any 1.1.2.0 0.0.0.255
```

Step 5: Apply the ACL.

#Apply the ACL 1001 on the interface vlan2 of Device1.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip policy-based-route 1001
Device1(config-if-vlan2)#exit
```

Step 6: Check the result.

#View the path that will pass to reach the destination entwork 1.1.1.0/24 through Traceroute on the PC.

```
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.
```

It can be viewed that the PC will pass Device1, Device3, and Device4 to reach the network 1.1.1.0/24.

#View the path that will pass to reach the destination network 1.1.2.0/24 through Traceroute on the PC.

```
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.
```

It can be viewed that the PC will pass Device1, Device2, and Device4 to reach the network 1.1.2.0/24.

Note

- Flexibly match the packets by the ACL rule. You can match the source IP address, destination IP address, source interface, destination interface, protocol, and TCP identifier information of the packet.
- The ACL can be bound on the L2/L3 Ethernet interface, VLAN, Interface VLAN, and globally.

6.15 PBR Tools

6.15.1 Overview

A routing 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 routing policy is mainly applied in the following aspects:

- Sets route properties: Sets the required route properties for the routes that

match the routing 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 improves the network security.
- Controls route redistribution: When a routing protocol redistributes external routes, it introduces only the routes that meet the requirements. A routing 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.

6.15.2 Configure PBR Tools

Table 861 Routing policy tool list

Configuration Tasks	
Configure a prefix list.	Configure a prefix list.
Configure an AS-PATH list.	Configure an AS-PATH list.
Configure a Community-list.	Configure a Community-list.
Configure an Extcommunity-list.	Configure an Extcommunity-list.
Configure a route map.	Create a route map.
	Configure the match clauses of a route map.
	Configure the set clauses of a route map.
Configure a key chain.	Configure a key chain.

6.15.2.1 Configure Prefix List

Configuration Condition

None

Configure a Prefix List

The prefix list filters routes based on prefixes. The ACL is first designed to filter data packets 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 862 Configure a prefix list

Step	Command	Description
Enter the 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*]	Mandatory. 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.

6. 15. 2. 2 Configure AS-PATH List

Configuration Condition

None

Configure an 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 863 Configure an AS-PATH list

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure an AS-PATH list.	ip as-path access-list *path-list-number* { permit | deny } *regular-expression*	Mandatory. 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 includes upper- and lower-case characters and numbers while metacharacters have special meanings, as shown in the following table.

Table 864 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.
?	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.

6.15.2.3 Configure Community-List

Configuration Condition

None

Configure a 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 865 Configure a community-list

Step	Command	Description
Enter the 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]	Mandatory. 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*	Mandatory. By default, no extended Community-list is configured.

6.15.2.4 Configure Extcommunity-List

Configuration Condition

None

Configure an 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 a Multi Protocol Label Switching (MPLS) Layer 3 Virtual Private Network (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 or 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 866 Configure an extcommunity-list

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure a standard Extcommunity-list.	ip extcommunity-list { *extcommunity-list-number* | standard *extcommunity-list-name*} { permit | deny } [rt *extcommunity-number* / soo *extcommunity-number*]	Mandatory. 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*	Mandatory. By default, no extended Extcommunity-list is configured.

6.15.2.5 Configure Route Map

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 Condition

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 a 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 867 Create a route map

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode.		
Create a route map.	route-map *map-name* [{ permit | deny } [*seq-number*]]	Mandatory. 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 a 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 868 Configure the match clause of a route map

Step	Command	Description
Enter the 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.
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	match metric	Optional.

that the route map matches.	*metric-value* [+-*offset*]	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 a 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 869 Configure the set clauses of a route map

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

Step	Command	Description
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.
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.
Configure the backup next hop	set fast-reroute [backup-interface *interface-names*] backup-nexthop *nexthop-address*	Optional By default, do not configure the route backup next hop.
Set the route next hop	set ip default next-hop *ip-address*	Optional.

Step	Command	Description
		By default, do not set the route next hop. When being used for the OSPF route re-distribution, set the route next hop.
Set the route next hop	set ip next-hop *ip-address*	Optional. By default, do not set the route next hop. When being used by BGP to associate the route map, set the route next hop.
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.
Configure 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 configured.
Set the tag option field of external routes.	set tag *tag-value*	Optional. By default, the tag option field

Step	Command	Description
		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.

6. 15. 2. 6 Configure Key Chain

Configuration Condition

None

Configure a 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 870 Configure a key chain

Step	Command	Description
Enter the global configuration mode.	configure terminal	-
Configure a key chain.	key chain *keychain-name*	Mandatory. By default, the key chain is not configured.
Configure a Key ID.	key *key-id*	Mandatory. By default, the key ID is not configured.
Configure a password.	key-string [0 | 7] *password*	Mandatory. 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 }	Mandatory. 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 }	Mandatory. By default, the transmit password is always valid.

6.15.2.7 Routing Policy Monitoring and Maintaining

Table 871 Routing policy monitoring and maintaining

Command	Description
clear ip prefix-list [*prefix-list-name network/length*]	Clears 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.
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.

6.15.3 PBT Tool Typical Configuration Example

6.15.3.1 Configure Route Redistribution with the Routing Policy

Network Requirements

- Run OSPF between Device1 and Device2, and run RIP between Device2 and Device3.

- On Device2, configure OSPF to redistribute RIP routes, and associate a routing 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

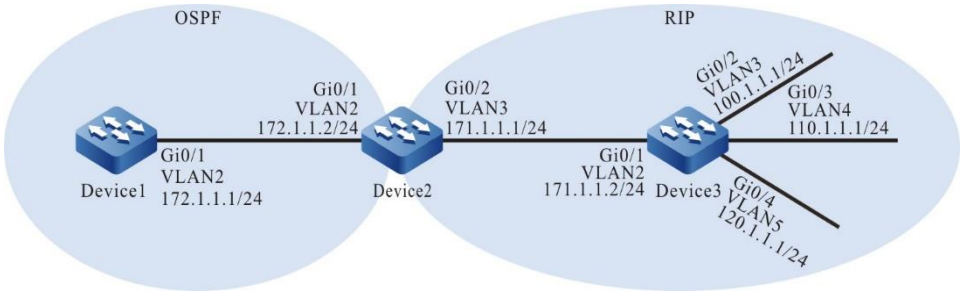


Figure 172 Configuring the route redistribution and associating the routing policy

Configuration Steps

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

Step 2: Configure the IP addresses of the interfaces. (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 redistribute RIP routes.

#Configure Device2.

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#Query the route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

OE  100.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE  110.1.1.0/24 [150/20] via 172.1.1.2, 00:49:57, vlan2
OE  120.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE  171.1.1.0/24 [150/20] via 172.1.1.2, 02:22:41, vlan2
```

According to the route table of Device1, the RIP routes 100.1.1.0/24, 110.1.1.0/24, and 120.1.1.0/24 are redistributed to the OSPF process and successfully advertised to Device1.

Step 6: Configure an ACL and routing 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)#commit
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)#commit
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)#commit
Device2(config-std-nacl)#exit
```

Configure routing 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 routing 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 redistribute RIP routes and associate a routing 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 route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

OE  100.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
OE  110.1.1.0/24 [150/50] via 172.1.1.2, 00:58:17, vlan2
OE  120.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
```

According to the OSPF database and route 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 redistributed into the target protocol.

6.15.3.2 Configure Routing Policy for BGP

Network Requirements

- Run IGP protocol ISPF 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 routing 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, reaches network segment 120.1.1.0/24 through Device2, and reaches network segment 130.1.1.0/24 through Device3.

Network Topology

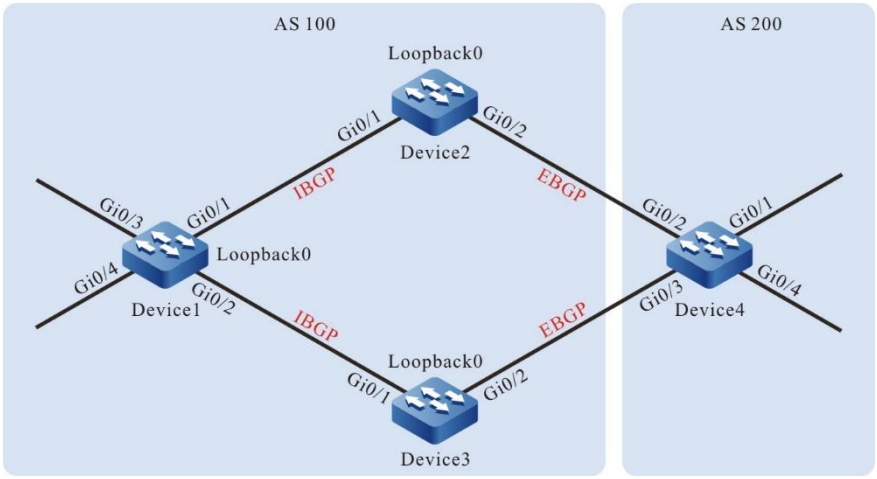


Figure 173 Configuring a routing policy for BGP

Device	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

Device	Interface	VLAN	IP Address
	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
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 the corresponding VLAN (omitted).

Step 2: Configure the IP addresses of the interfaces. (Omitted)

Step 3: Configure OSPF so that loopback routes are reachable between devices.

#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 route table of Device1.

```
Device1#show ip route ospf
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, E - IRMP, EX - IRMP external

O   39.1.1.1/32 [110/2] via 1.0.0.2, 19:11:33, vlan2
O   40.1.1.1/32 [110/2] via 2.0.0.2, 18:56:32, vlan3
```

#Query the route table of Device2.

```
Device2#show ip route ospf
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, E - IRMP, EX - IRMP external

O   2.0.0.0/24 [110/2] via 1.0.0.1, 19:19:10, vlan2
O   38.1.1.1/32 [110/2] via 1.0.0.1, 19:09:43, vlan2
O   40.1.1.1/32 [110/3] via 1.0.0.1, 18:56:49, vlan2
```

#Query the route table of Device3.

```
Device3#show ip route ospf
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, E - IRMP, EX - IRMP external

O   1.0.0.0/24 [110/2] via 2.0.0.1, 19:17:33, vlan2
O   38.1.1.1/32 [110/2] via 2.0.0.1, 19:09:59, vlan2
```

```
O   39.1.1.1/32 [110/3] via 2.0.0.1, 19:12:06, 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 advertises routes 120.1.1.0/24 and 130.1.1.0/24 to the BGP route 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 route 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 routing 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 route table of Device1.

```
Device1#show ip route bgp
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, E - IRMP, EX - IRMP external

B   100.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
B   110.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
```

According to the BGP route 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, so 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 routing 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 route table of Device4.

```
Device4#show ip route bgp
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, E - IRMP, EX - IRMP external

B   120.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3
B   130.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3
```

According to the BGP route 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, it takes longer time for Device2 to learn the two routes, so 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 routing 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 routing 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 routing 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 routing 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 routing 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 routing 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 a routing policy for BGP.

#Configure Device2.

Apply the routing policy lp to the outgoing routes of neighbor 38.1.1.1 and apply the routing 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 routing policy lp to the outgoing routes of neighbor 38.1.1.1 and apply the routing 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 routing 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 route table of Device1.

```
Device1#show ip route bgp
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, E - IRMP, EX - IRMP external

B   100.1.1.0/24 [200/0] via 39.1.1.1, 02:58:12, vlan2
B   110.1.1.0/24 [200/0] via 40.1.1.1, 02:58:10, vlan3
```

According to the BGP route 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 routing 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 route table of Device4.

```
Device4#show ip route bgp
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, E - IRMP, EX - IRMP external


B   120.1.1.0/24 [20/0] via 3.0.0.1, 03:05:39, vlan3
B   130.1.1.0/24 [20/0] via 4.0.0.1, 03:05:37, vlan4
```

According to the BGP route 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 routing 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.

7 Multicast

7.1 L2 Multicast Basics

7.1.1 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.

7.1.2 L2 Multicast Basics Function Configuration

Table 872 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 L2 static multicast	Configure L2 static multicast

7.1.2.1 Configure Unknown Packet Forwarding Policy of L2 Multicast

Unknown multicast service packets have two kinds of forwarding policies: drop unknown multicast service packets, or make the unknown multicast service packets flood.

Configuration Condition

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 873 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 Forwarding Policy of Unknown Multicast to Uplink Port

In the L2 multicast forwarding, the multicast service packet is forwarded through the L2 multicast forwarding table. When the multicast service packet does not match the forwarding table, it belongs to the unknown multicast service packet. If the function of discarding the unknown multicast service packet is enabled in the VLAN, the unknown multicast service packet will be discarded. At this time, after enabling the function of forwarding unknown multicast to the uplink port in the VLAN, the effect of flooding unknown multicast service packets to the uplink port can be realized.

Table 874 Configure the forwarding policy of the unknown multicast to the uplink port

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter VLAN configuration mode	vlan *vlan-id*	-
Configure the IP forwarding	l3-multicast drop-unknown	Mandatory

Step	Command	Description
policy of the L2 multicast		By default, the function of dropping the unknown multicast service packet is not enabled in VLAN.
Configure the MAC forwarding policy of the L2 multicast	l2-multicast drop-unknown	Mandatory By default, the function of dropping the unknown multicast service packet is not enabled in VLAN.
Configure the forwarding policy of the unknown multicast to the uplink port	multicast mrouter-forwarding	Optional By default, the function of dropping the unknown multicast service packet is not enabled in VLAN.

7.1.2.2 Configure the Policy of Checking Source MAC of L2 Multicast

It is used to configure whether to check the multicast source MAC.

Configuration Conditions

None

Configure the Policy of Checking Source MAC of L2 Multicast

By default, in the L2 multicast IP forwarding mode, the source MAC address of the multicast service packet needs to be checked. If there is an error, it will not be forwarded.

Table 875 Configure the policy of checking source MAC of the L2 multicast

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the policy of checking source MAC of the L2 multicast	multicast mismatch forward	Optional By default, do not enable the function of checking the source

Step	Command	Description
		MAC address of the L2 multicast.

7.1.2.3 Configure L2 Static multicast

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 Condition

Before configuring L2 static multicast, first complete the following task:

- Configure corresponding VLAN

Configure L2 static multicast

Table 876 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 link-aggregation *link-aggregation-id* { 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.

7.1.2.4 Monitoring and Maintaining of L2 Multicast Basis

Table 877 Monitoring and maintaining of L2 multicast basis

Command	Description
show l2-multicast ha { phase batch | phase flat | statistics }	Display the high reliability information of L2 multicast
show l2-multicast ip-entry	Display the IP forwarding table information of L2 multicast
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
show l2-multicast vlan-setting { all | *vlan-id* }	Display the L2 multicast VLAN information

7.1.3 Typical Configuration Example of L2 Static Multicast

7.1.3.1 Configure L2 Static Multicast

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

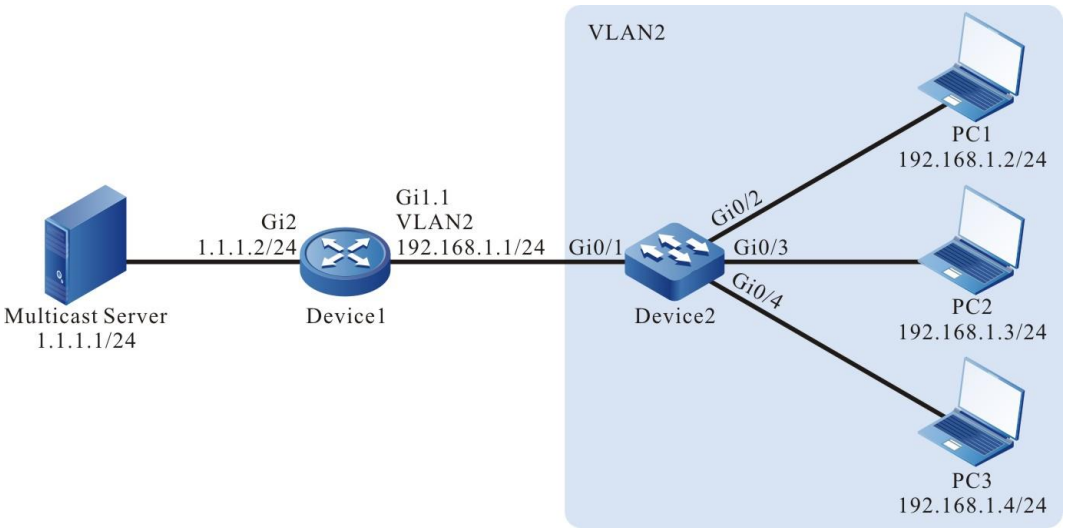


Figure 174 Network topology of configuring L2 static multicast

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 1 entries

---- -------- ----------------- ------------------------------
NO.  VID      Group MAC address  Interface Name
---- -------- ----------------- ------------------------------
1    2        0100.5E01.0101     [M] gi0/2
                                 [F] gi0/3
```

#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.

7.1.3.2 Configure IPv6 L2 Static Multicast

Network Requirements

- Device1 configures IPv6 multicast routing protocol; Device2 configures IPv6 L2 static multicast in VLAN2; PC1 is the receiver of multicast service; PC2 and PC3 are the receiver of non-multicast service.
- Multicast Server sends IPv6 multicast service packets; PC1 can receive multicast service packets correctly; PC2 and PC3 cannot receive multicast service packets.

Network Topology

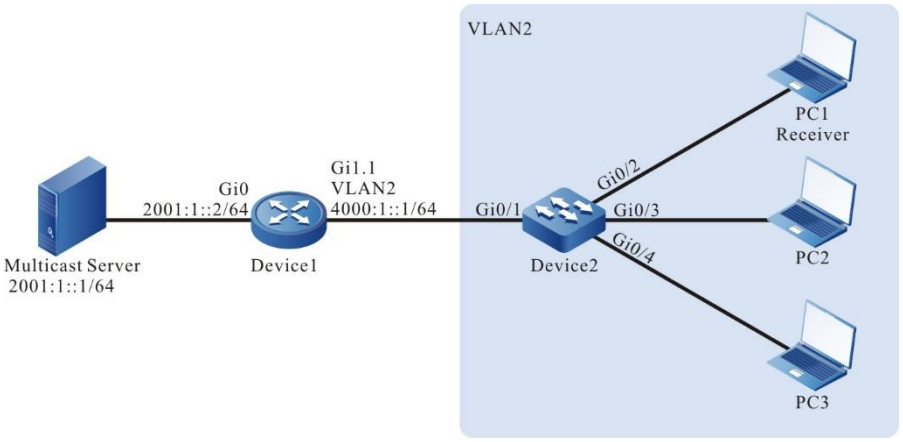


Figure 175 Network topology of configuring IPv6 L2 static multicast

Configuration Steps

Step 1: Device1 configures interface IP address and enables multicast routing protocol. (omitted)

Step 2: Configure Device2.

#On Device2, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of ports gigabitethernet0/2~gigabitethernet0/4 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
```

#On Device2, configure the link type of port gigabitethernet0/1 as Trunk, permit the services of VLAN2 to pass, and 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
```

#In VLAN2, enable the unknown multicast dropping.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Configure the members of the L2 static multicast group.

```
Device2(config)# l2-multicast mac-entry static 3333.0000.0001 vlan 2
Device2(config-mcast)#interface gigabitethernet 0/2 member
Device2(config-mcast)#interface gigabitethernet 0/3 forbidden
Device2(config-mcast)#exit
```

Step 3: Check the result.

#Query the IPv6 L2 static multicast entries of Device2.

```
Device2# show l2-multicast mac-entry static
Current L2 Static Multicast 1 entries

---- -------- ----------------- ------------------------------------------
NO.  VID      Group MAC address  Interface Name
---- -------- ----------------- ------------------------------------------
1    2        3333.0000.0001     [M] gi0/2
                                 [F] gi0/3
```

#Multicast Server sends the multicast packet with the destination address ff10::1. PC1 can correctly receive the multicast packet, but PC2 and PC3 cannot receive the multicast packets.

Note

- In IPv6 L2 static multucast, the multicast packets can only be forwarded to the port whose role is member.
- For the forbidden port, even being added to the multicast group of the static multicast group by the mld snooping mode, the multicast packets whose destination address is the static multicast group will not be forwarded to the forbidden port.
- The non-member and non-forbidden ports can be added to the multicast group of the static multicast group by the mld snooping mode, and the multicasy packet whose destination address is the static multicast group will be forwarded to the port.

7.2 IGMP snooping

7.2.1 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.

7.2.2 IGMP snooping Function Configuration

Table 878 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 L2 forwarding function
Configure IGMP snooping querier	Enable the IGMP snooping querier
	Configure the source IP address of the IGMP

Configuration Task	
	query packet
	Configure general group query interval
	Configure the maximum response time
	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

7.2.2.1 Configure IGMP snooping Basic Functions

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 Condition

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 879 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 880 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 L2 Forwarding

Usually, IGMP snooping forwards the multicast service packet in VLAN according to the multicast source IP address and multicast destination IP address. After configuring IGMP snooping L2 forwarding, IGMP snooping forwards multicast service packets in VLAN according to the multicast destination MAC address.

Table 881 IGMP snooping L2 forwarding

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable L2 multicast L2 forwarding function in the specified VLAN	ip igmp snooping vlan *vlan-id* l2-forwarding	Mandatory By default, IP forwarding function of VLAN IGMP snooping L2 multicast of 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.

Caution

- Because 32 multicast IP addresses correspond to one multicast MAC

address, and L2 forwarding can't specify multicast source forwarding, there may be multiple IP multicast source groups corresponding to the same MAC group. At this time, there will be forwarding conflict.

7.2.2.2 Configure IGMP snooping Querier

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 Condition

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 882 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 883 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 884 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.

Table 885 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 “last life period”, delete the information of the multicast group.

Table 886 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 887 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.

7.2.2.3 Configure IGMP snooping Router Port

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 Condition

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 888 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-*	Mandatory By default, the IGMP snooping

Step	Command	Description
	name | link-aggregation *link-aggregation-id* }	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 889 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.

7.2.2.4 Configure IGMP snooping TCN Event

Configuration Condition

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 spanning tree 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, making the fast convergence.

After enabling IGMP snooping TCN event fast convergence, non-spanning tree root port also actively sends the global IGMP leave packet (group address: 0.0.0.0), making the fast convergence.

Table 890 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 891 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 892 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.

7.2.2.5 Configure IGMP snooping Policy

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 Condition

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 893 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

Step	Command	Description
		refused multicasts group is not configured.
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	interface 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 894 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	interface 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 6144.

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 895 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. 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	interface link-aggregation *link-aggregation-id*	
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.

Configure Interface to Control PIM JOIN Packet

After configuring the interface to control PIM JOIN packet, the JOIN packet is forwarded by software, not by hardware.

Table 896 Configure the interface to control PIM JOIN packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the interface to control PIM JOIN packet	ip igmp snooping vlan *vlan-id* ctrl-pim	Mandatory By default, do not control the PIN JOIN packet of the

Step	Command	Description
		specified VLAN.

Note

- Before enabling, flood the JOIN packet in VLAN. After enabling, the packet is forwarded to CPU, but will not flood in VLAN.

7.2.2.6 Configure IGMP Snooping Proxy

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 Condition

Before configuring the IGMP snooping proxy function, first complete the following task:

- Enable global and VLAN IGMP snooping function

Configure IGMP Snooping Proxy

Table 897 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 {	Mandatory By default, IGMP agent port is

Step	Command	Description
	interface-name | link-aggregation *link-aggregation-id* }	not configured in VLAN.

7.2.2.7 Configure IGMP snooping Static Group

IGMP snooping static group is the static IGMP snooping groups table entries generated by static configuration. By configuring IGMP snooping static group, we can effectively solve the aging problem of IGMP snooping dynamic learning multicast group.

When the device is configured with IGMP snooping static group in VLAN, IGMP snooping querier and querier address in VLAN, and IGMP snooping proxy port in VLAN, the device will send IGMP member report packet to IGMP snooping proxy port in VLAN when generating static IGMP snooping groups table entry. The source IP address of the IGMP member report packet is the configured querier address. In this way, the uplink router can correctly maintain IGMP membership table. When the IGMP snooping static group configuration in the VLAN is deleted, the device will delete the corresponding IGMP snooping static group table entry and send the IGMP member leave packet to the IGMP snooping proxy port in the VLAN.

Configuration Condition

Before configuring the IGMP snooping static group function, first complete the following task:

- Enable global and VLAN IGMP snooping function
- Add port members in VLAN.

Configure IGMP snooping Static Group

Table 898 Configure IGMP snooping static group

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure IGMP snooping static group	ip igmp snooping vlan *vlan-id* static-group *group-ip-address* { interface *interface-name* | interface link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure IGMP snooping static group.

7.2.2.8 IGMP snooping Monitoring and Maintaining

Table 899 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* | interface 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
show ip igmp snooping interface statistics	Configure the statistics information of the

Command	Description
	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* [interface *interface-name* | interface link-aggregation *link-aggregation-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* | interface link-aggregation *link-aggregation-id*]	Display the information of the L2 multicast control

7.2.3 Typical Configuration Example of IGMP snooping

7.2.3.1 Configure IGMP snooping

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

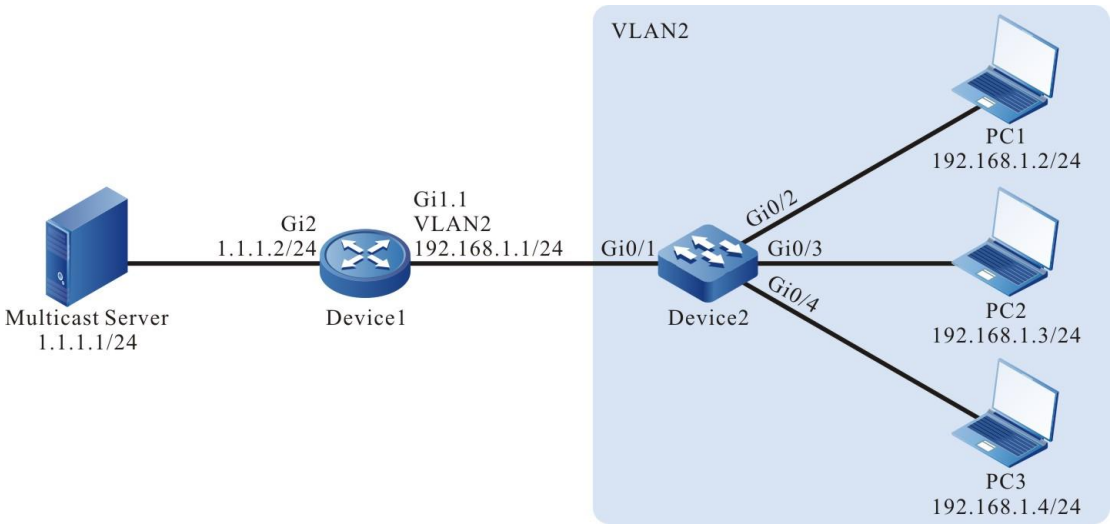


Figure 176 Network topology of IGMP snooping

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  192.168.1.2  stopped          00:00:55
2        gi0/3        224.1.1.1    00:03:44  192.168.1.3  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.

7.2.3.2 Configure Multicast Receiving Control

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

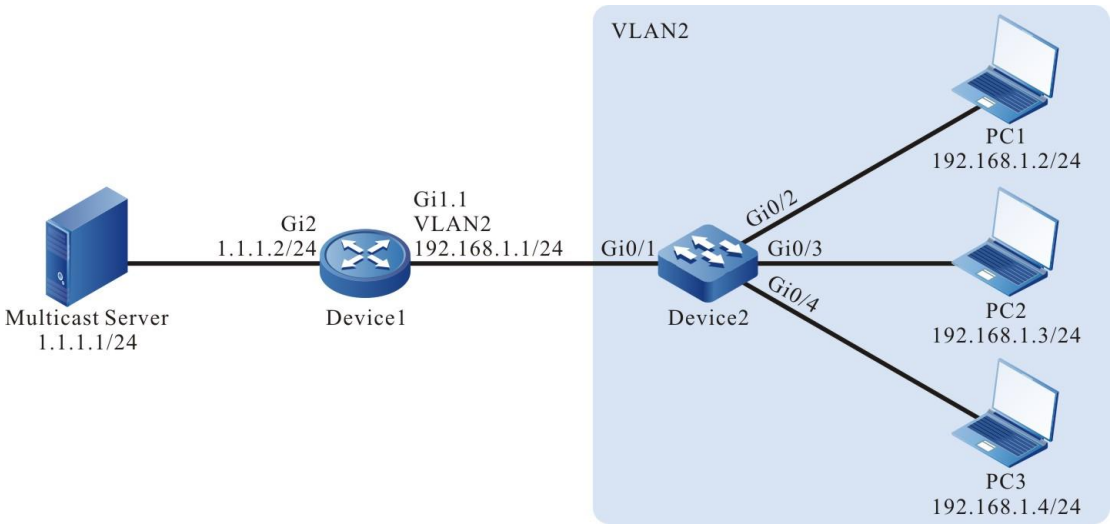


Figure 177 Network topology of configuring multicast receiving control

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)#permit all
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.

7.2.3.3 Configure IGMP Snooping Proxy

Network Requirements

- On Device1, configure multicast routing protocol.
- On Device2, enable 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

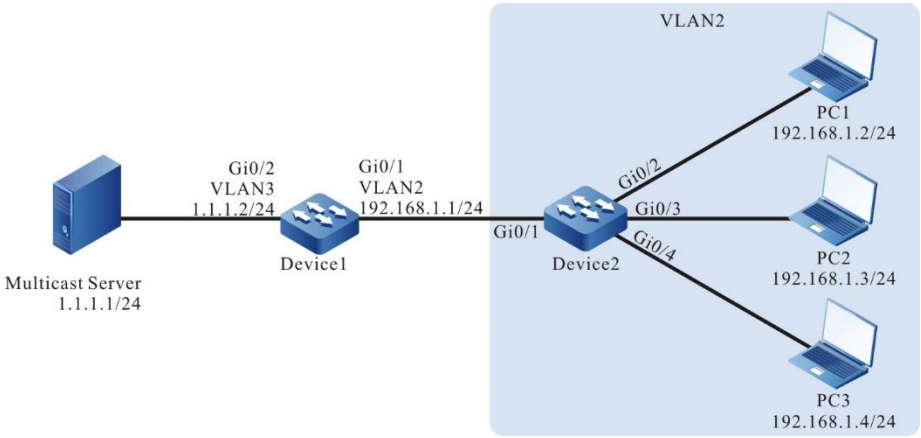


Figure 178 Network topology of configuring IGMP snooping proxy

Configuration Steps

Step 1: Device1 configures the interface IP address and enables the multicast route protocol.

```
n2)# ip pim sparse-mode
Device1(config-if-vlan2)# exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)# ip address 1.1.1.2 255.255.255.0
Device1(config-if-vlan3)# ip pim sparse-mode
Device1(config-if-vlan3)# 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
```

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 report source address          : 192.168.1.254
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    V2 Expires
224.1.1.1        vlan 2            00:00:15 00:04:11 192.168.1.254     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     00:03:54 192.168.1.254  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    V2 Expires
224.1.1.1        vlan 2            00:06:48 00:03:48 192.168.1.2      stopped
```

After PC1 and PC2 leaves multicast group 224.1.1.1, PC3 does not leave the multicast group, and there are 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.

7.2.3.4 Configure Unknown Multicast Re-direction

Network Requirements

- Device2 configures multicast routing protocol.
- Device1 enables IGMP snooping, unknown multicast dropping, and unknown multicast re-direction.
- Multicast Server sends the multicast service packet; PC1, PC2, and PC3 can correctly receive the multicast service packet.

Network Topology

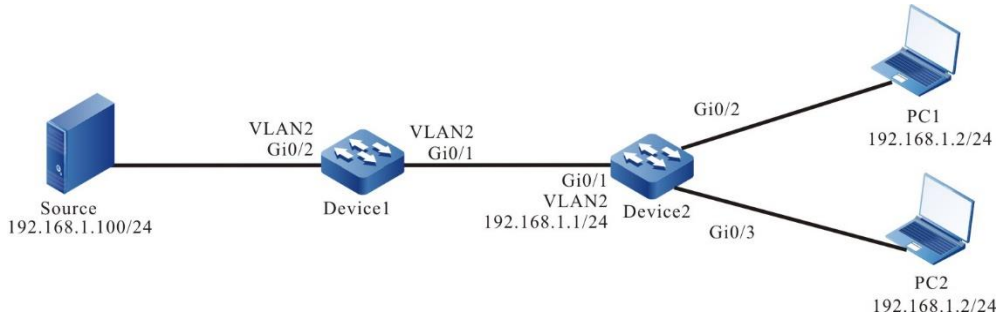


Figure 179 Network topology of configuring unknown multicast re-direction

Configuration Steps

Step 1: Configure the IP address of Device2 interface, and enable the multicast route protocol. (omitted)

Step 2: Configure Device2 and Device1.

#On Device2, configure the link type of port gigabitethernet0/2-gigabitethernet0/3 as Access, permitting VLAN2 services to pass, configure the link type of port gigabitethernet0/1 as trunk, permitting VLAN2 service to pass, and configure PVID as 1.

```
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
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
```

#On Device1, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device1, configure the link type of port gigabitethernet0/2 as Access, permitting VLAN2 services to pass, configure the link type of port gigabitethernet0/1 as trunk, permitting VLAN2 service to pass, and configure PVID as 1.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)# switchport access vlan 2
Device1(config-if-gigabitethernet0/2)#exit
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)#switchport trunk pvid vlan 1
Device1(config-if-gigabitethernet0/1)#exit
```

#In VLAN2, enable unknown multicast dropping.

```
Device1(config)#vlan 2
Device1(config-vlan2)#l2-multicast drop-unknown
Device1(config-vlan2)#exit
```

#Enable IGMP snooping.

```
Device1(config)#ip igmp snooping
Device1(config)#ip igmp snooping vlan 2
```

#In VLAN2, enable unknown multicast re-direction.

```
Device1(config)#vlan 2
Device1(config-vlan2)#multicast mrouter-forwarding
Device1(config-vlan2)#exit
```

Step 3: Check the result.

#PC1 and PC2 send IGMPv2 member report packets to join multicast group 224.1.1.1.

#Query the multicast member table of Device2.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface       Uptime    Expires   Last Reporter   V1 Expires  V2 Expires
224.1.1.1       vlan2           00:21:02  00:03:47  192.168.1.2     stopped
```

#Multicast server sends the multicast service packet whose destination address is 224.1.1.1.

```
#PC1 and PC2 can correctly receive the multicast packets.
```

7.2.3.5 Configure IGMP snooping Static Group

Network Requirements

- Device 1 is configured with multicast routing protocol. Device 2 enables

IGMP snooping in VLAN 2. PC1 and PC2 are receivers of IGMP snooping static group service and PC3 is the receiver of non-multicast service.

- Multicast server sends multicast service packets, PC1 and PC2 can receive multicast service packets correctly, and PC3 cannot receive multicast service packets.

Network Topology

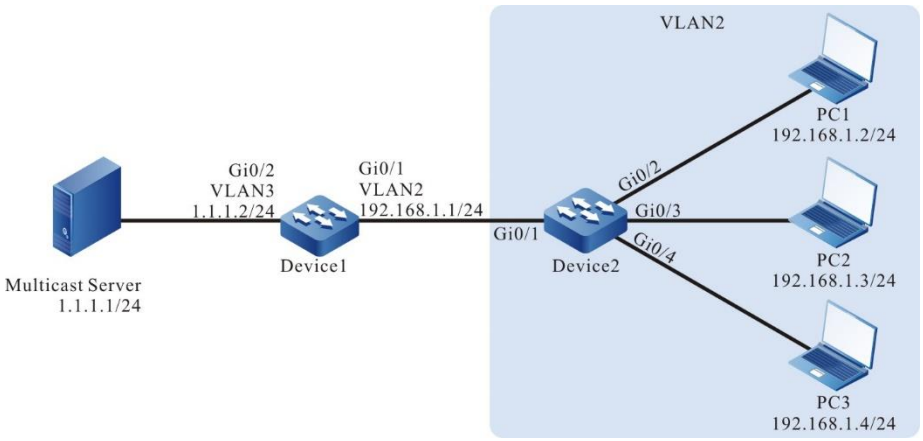


Figure 180 Network topology of configuring IGMP snooping static group

Configuration Steps

Step 1: On Device1, configure the interface IP address, and enable multicast routing protocol (omitted).

Step 2: Configure Device2.

#On Device2, create VLAN2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of ports gigabitethernet0/2~gigabitethernet0/4 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
```

#On Device2, configure the link type of ports gigabitethernet0/1 as Trunk, permitting the services of VLAN2 to pass, and configured 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
```

#In VLAN2, enable unknown multicast dropping.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#l3-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable IGMP snooping, and configure IGMP snooping static group.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 2 static-group 224.1.1.1 interface gigabitethernet 0/2
Device2(config)#ip igmp snooping vlan 2 static-group 224.1.1.1 interface gigabitethernet 0/3
Device2(config)#exit
```

Step 3: Check the result.

#View the multicast member table of Device2.

```
Device2#show ip igmp snooping groups
IGMP Snooping Static Group Membership
Total 2 group

VLAN ID  Port Name         Group Address   Uptime
_______ ___________________ _____________ _________
2       gi0/2             224.1.1.1       00:00:48
2       gi0/3             224.1.1.1       00:00:45
```

#Multicast Server sends the multicast service packet with the destination address of 224.1.1.1. PC1 and PC2 can receive the multicast service packets correctly, and PC3 cannot receive the multicast service packets.

7.3 Multicast VLAN

7.3.1 Overview

For the traditional multicast-on-demand mode, when in the user-on-demand of

different VLANs, each VLAN copies one multicast flow in the VLAN. The multicast-on-demand mode wastes lots of bandwidth.

To solve the problem, you can configure the multicast VLAN mode to make the users in different VLANs share one multicast VLAN. After the multicast VLAN function is enabled, the multicast flow is just transmitted in the multicast VLAN and the multicast VLAN is completely separated from the user VLAN. This not only saves the bandwidth, but also ensures the security.

Multicast VLAN has two kinds: MVR (Multicast VLAN Registration) and MVP (Multicast VLAN Plus).

7.3.2 Multicast VLAN Configuration

Table 900 Multicast VLAN configuration list

Configuration Task	
Configure MVP	Configure MVP multicast VLAN
	Enable the MVP function
Configure MVR	Configure MVR multicast VLAN
	Enable the MVR function

7.3.2.1 Configure MVP

MVP is used by the edge network. Sub VLAN member port can connect to multicast device and also can directly connect to the user. When connecting to the multicast device, sub VLAN member port sends the multicast packet with VLAN Tag; when connecting to the user, sub VLAN member port can send multicast packet without VLAN Tag.

Configuration Condition

Before configuring MVP multicast VLAN, first complete the following task:

- Configure VLAN
- Enable global and VLAN IGMP snooping function

Configure MVP multicast VLAN

Configure MVP to realize the cross-VLAN forwarding multicast packet between MVP multicast VLAN and member sub VLAN. The member port of the MVP multicast VLAN needs to be consistent with the VLAN Tag of the connected upstream device; the MVP sub VLAN member port needs to be consistent with the VLAN Tag of the connected downstream device.

Table 901 Configure MVP multicast VLAN

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the MVP multicast VLAN	multicast-vlan *mvlan-id* subvlan *subvlan-id*	Mandatory By default, the MVP multicast VLAN and member sub VLAN are not configured.

Enable MVP Function

After enabling the MVP function in the MVP multicast VLAN, the cross-VLAN forwarding packet between the MVP multicast VLAN and member sub VLAN can be realized.

Table 902 Enable the MVP function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter VLAN configuration mode	vlan *vlan-id*	-
Enable the MVP function in VLAN	multicast-vlan enable	Mandatory By default, the MVP function is disabled in VLAN.

7.3.2.2 Configure MVR

MVR is used by the edge network. MVR multicast VLAN member port can only connect to users, and multicast packets sent from VLAN member port cannot have

VLAN tag.

Configuration Condition

Before configuring MVR multicast VLAN, first complete the following task:

- Configure VLAN
- Enable global and VLAN IGMP snooping function

Configure MVR Multicast VLAN

When multiple user ports belong to different VLANs, users in different VLANs can share a multicast VLAN by adding these ports to MVR multicast VLAN.

Table 903 Configure MVR multicast VLAN

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure MVR multicast VLAN	mvr vlan *vlan-id*	Mandatory By default, do not configure the MVR multicast VLAN.

Enable the MVR Function

When MVR function is enabled, the configuration of MVR multicast VLAN will take effect.

Table 904 Enable the MVR function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the MVR function	mvr enable	Mandatory By default, do not enable the MVR function.

7.3.2.3 Multicast VLAN Monitoring and Maintaining

Table 905 Multicast VLAN monitoring and maintaining

Command	Description
show multicast-vlan vlan-id	Display the MVP multicast VLAN information
show mvr	Display the MVR information

7.3.3 Typical Configuration Example of Multicast VLAN

7.3.3.1 Configure MVP

Network Requirements

- Device1 configures the multicast route protocol.
- Device2 enables IGMP snooping and configures MVP.
- Multicast Server sends multicast service packets; multicast VLAN2 can copy the multicast service packets to sub VLAN4-VLAN5. PC1, PC2 and PC3 can correctly receive the multicast service packets.

Network Topology

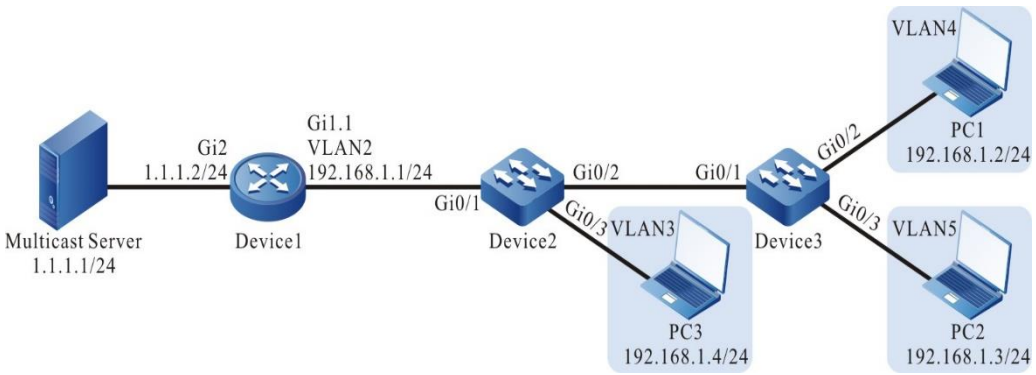


Figure 181 MVP typical configuration networking

Configuration Steps

Step 1: Device1 configures the interface IP address and enables the multicast route protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2-VLAN5 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-5
```

#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
```

#Configure the link type of port gigabitethernet0/2 on Device2 as Trunk, permitting the services of VLAN4-VLAN5 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode trunk
Device2(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 4-5
Device2(config-if-gigabitethernet0/2)# switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device2 as Access, permitting the services of VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport access vlan 3
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 3
Device2(config)#ip igmp snooping vlan 4
Device2(config)#ip igmp snooping vlan 5
```

#Configure MVP.

```
Device2(config)#multicast-vlan 2 subvlan 3-5
Device2(config)#vlan 2
Device2(config-vlan2)#multicast-vlan enable
Device2(config-vlan2)#exit
```

Step 3: Configure Device3.

#Create VLAN4-VLAN5 on Device3.

```
Device3#configure terminal
Device3(config)#vlan 4-5
```

#Configure the link type of port gigabitethernet0/1 on Device3 as Trunk, permitting the services of VLAN4-VLAN5 to pass; PVID is configured as 1.

```
Device3(config)#interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#switchport mode trunk
Device3(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 4-5
Device3(config-if-gigabitethernet0/1)# switchport trunk pvid vlan 1
Device3(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2 on Device3 as Access, permitting the services of VLAN4 to pass.

```
Device3(config)#interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/2)#switchport access vlan 4
Device3(config-if-gigabitethernet0/2)#exit
```

#Configure the link type of port gigabitethernet0/3 on Device3 as Access, permitting the services of VLAN5 to pass.

```
Device3(config)#interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/3)#switchport access vlan 5
Device3(config-if-gigabitethernet0/3)#exit
```

Step 4: Check the result.

#View the MVP information.

```
Device2#show multicast-vlan
Multicast Vlan Table
--------------------------------
VLAN ID: 2
status: enable
subvlan count: 3
subvlan: 3-5
```

#PC1, PC2, and PC3 send the IGMPv2 member relation report to add to multicast group 224.1.1.1.

#View the multicast member table of Device2.

```
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
------------------------------------------------------------------------------ ---------
3       gi0/3        224.1.1.1     00:03:54  192.168.1.4  stopped          00:01:18
```

```
4       gi0/2       224.1.1.1    00:04:17  192.168.1.2  stopped        00:00:07
5       gi0/2       224.1.1.1    00:03:54  192.168.1.3  stopped        00:01:21
```

#View the multicast forwarding table of Device2.

```
Device2#show ip igmp snooping l3_ip_table
Total 1 entry

Flags: M - L2 multicast, S - short of resources

(*, 224.1.1.1)
  Ingress Vlan: 2
  Flags      : M
  L2 Interface List: gigabitethernet0/1
    Egress Vlan  Flags  L3 Interface List
    3            M      gigabitethernet0/3
4           M      gigabitethernet0/2
5           M      gigabitethernet0/2
```

#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.

7.3.3.2 Configure MVR

Network Requirements

- Device1 configures the multicast route protocol.
- There are three VLANs in the whole network, vlan2 - vlan4. The port connecting the PC joins the corresponding VLAN in hybrid mode.
- Device2 enables IGMP snooping and configures MVP.
- Multicast Server sends multicast service packets; PC1, PC2 and PC3 can correctly receive the multicast service packets.

Network Topology

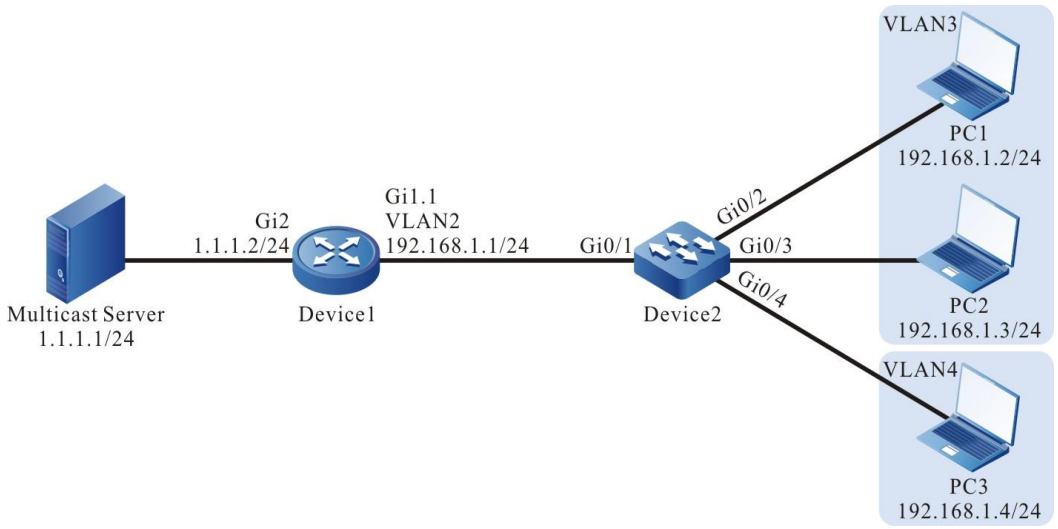


Figure 182 MVR typical configuration networking

Configuration Steps

Step 1: Device1 configures the interface IP address and enables the multicast route protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2-VLAN4 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2-4
```

#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 hybrid
Device2(config-if-gigabitethernet0/1)#switchport hybrid tagged vlan 2
Device2(config-if-gigabitethernet0/1)# switchport hybrid pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Configure the link type of port gigabitethernet0/2-gigabitethernet0/3 on Device2 as Hybrid, permitting the services of VLAN2-VLAN3 to pass; PVID is configured as 3.

```
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#switchport mode hybrid
Device2(config-if-range)#switchport hybrid untagged vlan 2-3
Device2(config-if-range)#switchport hybrid pvid vlan 3
```

```
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/4 on Device2 as Hybrid, permitting the services of VLAN2 and VLAN4 to pass; PVID is configured as 4.

```
Device2(config)#interface gigabitethernet 0/4
Device2(config-if-gigabitethernet0/4)#switchport mode hybrid
Device2(config-if-gigabitethernet0/4)#switchport hybrid untagged vlan 4
Device2(config-if-gigabitethernet0/4)#switchport hybrid untagged vlan 2
Device2(config-if-gigabitethernet0/4)#switchport hybrid pvid vlan 4
Device2(config-if-gigabitethernet0/4)#exit
```

#Configure IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 3
Device2(config)#ip igmp snooping vlan 4
```

#Configure MVR.

```
Device2(config)#mvr vlan 2
Device2(config)#mvr enable
Device2(config)#exit
```

Step 3: Check the result.

#Query the MVR information.

```
Device2#show mvr
 MVR status:enable
 multicast-vlan: 2
```

#PC1, PC2, and PC3 send the IGMPv2 member relation report to add to multicast group 224.1.1.1.

#View the multicast member table of Device2.

```
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   00:04:14  192.168.1.2  stopped       00:00:07
2     gi0/3      224.1.1.1   00:04:14  192.168.1.3  stopped       00:00:07
2     gi0/4      224.1.1.1   00:04:14  192.168.1.4  stopped       00:00:07
```

#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.

7.4 IPv4 Multicast Basics

7.4.1 Overview

IPv4 multicast basics is the basis of running the IP multicast protocol and the common part of all multicast protocols. No matter which multicast route protocol runs, we first need to enable the IP multicast forwarding function so that the device can forward the multicast service packets.

7.4.2 Basic Function Configuration of IPv4 Multicast

Table 906 Basic function configuration list of IPv4 multicast

Configuration Task	
Enable IP multicast forwarding	Enable the IP multicast forwarding
Configure IP multicast forwarding rule	Configure the multicast forwarding management edge
	Configure the multicast forwarding entry limitation

Caution

- L3 Ethernet interface does not support IP multicast forwarding rule function.

7.4.2.1 Enable IP Multicast Forwarding

Configuration Condition

No

Enable IP Multicast Forwarding

Enable the IP multicast forwarding function so that the forwarding multicast service can run normally.

Table 907 Enable IP multicast forwarding

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable IP multicast forwarding	ip multicast-routing [vrf *vrf-name*]	Mandatory By default, the IP multicast forwarding is not enabled.

7.4.2.2 Configure IP Multicast Forwarding Rule

Configuration Condition

Before configuring the multicast forwarding management edge of the interface, first complete the following task:

- Configure interface IP address, making the neighboring node network layer reachable
- Enable IP multicast forwarding
- Configure multicast route protocol

Configure Multicast Forwarding Management Edge

After configuring the management edge, the device can filter the multicast service packets and the multicast service packets not matching the access list rules cannot be forwarded from the interface.

Table 908 Configure multicast forwarding management edge

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure multicast forwarding	ip multicast boundary { *access-list-number* | *access-list-name* }	Mandatory By default, the multicast

Step	Command	Description
management edge		forwarding management edge is not configured.

Configure Multicast Forwarding Entry Timeout

Configure the timeout of the multicast forwarding entry. After timeout, delete or perform other operations by the entry tag.

Table 909 Configure the timeout of the multicast forwarding entry

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the timeout of the multicast forwarding entry	ip multicast mrt-timer *timevalue*	Optional By default, the timeout of the multicast forwarding entry is 180s.

Configure Multicast Forwarding Entry Limitation

Configure the maximum number of the multicast forwarding entries. After exceeding the maximum number of the multicast forwarding entries, the new multicast forwarding entry is not created.

Table 910 Configure multicast forwarding entry limitation

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure multicast forwarding entry limitation	ip multicast route-limit *number-value* [vrf *vrf-name*]	Optional By default, the maximum number of the multicast forwarding entries is 6144. The value range varies with the system work mode.

7.4.2.3 Monitoring and Maintaining of IPv4 Multicast Basics

Table 911 Monitoring and maintaining of IPv4 multicast basics

Command	Description
clear ip mcache [source *source-ip-address*] [group *group-ip-address*] [all | vrf *vrf-name*]	Clear the multicast route entry
show ip mcache [source *source-ip-address*] [group *group-ip-address*] [vrf *vrf-name*]	Display the multicast route table information
show ip mnhp [[vrf *vrf-name*] | [vlan *vlan-id*]]	Display the multicast next-hop information
show ip mvif [vrf *vrf-name*]	Display the multicast virtual interface information
show ip mvrf	Display the multicast VRF information

7.5 IGMP

7.5.1 Overview

IGMP (Internet Group Management Protocol) is the protocol for managing the IP multicast members in the TCP/IP protocol stack, used to set up and maintain the multicast group member relation between the IP host and the direct neighboring multicast device.

IGMP has three versions. Currently, the widely-used is IGMPv2. IGMPv2 has three kinds of packets: query packets, group member relation report and group member leave packet.

Query packet includes the general query packet and the specified group query packet. The device gets to know which members there are in the direct-connected network via the general query packets and whether there are the members of one specified group in the direct-connected network via the specified group query packets.

Group member relation report: When the host wants to add into one multicast group, the host immediately sends the group member relation report to the desired multicast group. When the host receives one query packet, it also sends the group

member relation report.

Group member leave packet: When the host leaves one multicast group, send one group member leave report. When the device receives the group member leave packet, send the specified group query to confirm whether one specified group has members.

7.5.2 IGMP Function Configuration

Table 912 IGMP function configuration list

Configuration Task	
Configure IGMP basic functions	Enable the IGMP protocol
	Configure the IGMP version
	Configure static group adding
	Configure multicast group filter
	Configure SSM multicast group filter
Adjust and optimize the IGMP network	Configure the query interval of the general group
	Configure the robustness factor
	Configure the maximum response time
	Configure the specified group query
	Configure the other querier timeout
	Configure the fast leave

Caution

- L3 Ethernet interface does not support the IGMP function.

7.5.2.1 Configure IGMP Basic Functions

Configuration Condition

Before configuring the IGMP basic functions, first complete the following task:

- Configure the interface network layer address, making the neighboring

node network layer reachable

Enable IGMP Protocol

Table 913 Enable the IGMP protocol

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the IP multicast forwarding	ip multicast-routing	Mandatory By default, the IP multicast forwarding is disabled.
Enter interface configuration mode	interface *interface-name*	-
Enable the IGMP protocol	ip pim sparse-mode	Mandatory By default, IGMP is disabled. When the interface enables the multicast route protocol, automatically enable IGMP. Only after enabling IGMP, all IGMP configurations can take effect.

Configure IGMP Version

Table 914 Configure the IGMP version

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the IGMP version	ip igmp version *version-number*	Mandatory By default, the IGMP version is 2.

Note

- Because the packet structure and kind of different versions of IGMP protocols are different, it is suggested to configure the same version of IGMP for all devices on the same subnet.

Configure Static Group Adding

After configuring one static group or source group in the interface, the device regards that the interface has the receiver of the multicast group or source group.

Table 915 Configure static group adding

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the static group adding	ip igmp static-group *group-ip-address* [*source-ip-address*]	Mandatory By default, the interface is not added to any multicast group or source group in the static mode.

Configure Multicast Group Filter

The interface configured with the IGMP multicast group filter filters the group member relation report in the segment according to the ACL rules and only the group member relation report permitted by ACL is processed and the un-permitted is directly dropped. For the existing but not permitted by ACL multicast group, immediately delete the multicast group information.

Table 916 Configure multicast group filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-

Step	Command	Description
Configure the IGMP multicast group filter	ip igmp access-group { *access-list-number* | *access-list-name* }	Mandatory By default, the multicast group filter is not configured.

Note

- **ip igmp access-group** Command only supports the standard ACL.

Configure SSM Multicast Group Filter

After configuring the range of the source groups received by IGMP, filter the received source group member relation report to limit the source group range the interface serves. For the groups belonging to the PIM-SSM range, only not the (IS_EX, TO_EX) member relation report of IGMPv3 permitted by the access list (S, G) can be accepted.

Table 917 Configure the SSM multicast group filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the SSM multicast group filter	ip igmp ssm-access-group { *access-list-number* | *access-list-name* }	Mandatory By default, do not filter to limit the SSM group members.

Note

- **ip igmp ssm-access-group** can take effect only when the interface enables IGMPv3.
- **ip igmp ssm-access-group** takes effect only for the source groups in the

PIM SSM range.

- **ip igmp ssm-access-group** only supports the extended ACL.

7.5.2.2 Adjust and Optimize IGMP Network

Configuration Condition

Before adjusting and optimizing the IGMP network, first complete the following task:

- Configure interface network layer address, making the neighboring node network layer reachable
- Enable the IGMP protocol

Configure Query Interval of General Group

IGMP querier periodically sends the general group query packets 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.

Table 918 Configure the query interval of the general group

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the query interval of the general group	ip igmp query-interval *interval-value*	Optional By default, the interval of sending the IGMP general group query packets is 125s.

Note

- The genera query intervals of the devices on the same segment should try to keep consistent.

Step	Command	Description

- The general group query interval should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

Configure Robustness Factor

Table 919 Configure robustness factor

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the robustness factor	ip igmp robustness-variable *variable-value*	Optional By default, the robustness factor of the IGMP querier is 2.

Note

- After configuring the robustness factor, the following parameters also change with the robustness parameters:
- Group member timeout = Robustness factor * general group query time + maximum response time;
- Other querier timeout = Robustness factor * general query time + maximum response time/2;
- The larger the robustness factor, the larger the IGMP group member timeout and other querier timeout. The user sets the value according to the actuality of the network.

Configure Maximum Response Time

The general group query packet sent by the IGMPv2 querier contains the maximum response time field and the receiver sends the group member relation report within the maximum response interval.

Table 920 Configure the maximum response time

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the maximum response time	ip igmp query-max-response-time *seconds*	Optional By default, the maximum response time of the IGMP general group query is 10s.

Configure Specified Group Query

After the IGMP querier receives the leave packet of one multicast group, send the specified group query packets of the "specified group query times" times to query the multicast group on the segment, so as to know whether the subnet has the members of the multicast group. If not receiving the member relation report of the multicast group after waiting for "last life period", delete the information of the multicast group.

Table 921 Configure the specified group query

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the query interval of the specified group	ip igmp last-member-query-interval *interval-value*	Optional By default, the interval of sending the specified group query

Step	Command	Description
		packets is 1s.
Configure the query times of the specified group	ip igmp last-member-query-count *count-value*	Optional By default, the time of sending the specified group query packets is 2.

Note

- **ip igmp last-member-query-interval** and **ip igmp last-member-query-count** are invalid in IGMPv1, because the IGMPv1 host does not send leave packets when leaving one multicast group.

Configure Other Querier Timeout

The device with the smallest address in one subnet is elected as the querier and the other devices are called non-querier. On the non-queriers, set one timeout as the timer of "other querier timeout" (the other queriers have timer) for the querier. When the non-querier receives the query packet of the querier, refresh the timer. When the timer times out, it indicates that the current IGMP querier becomes invalid and you need to re-elect the new querier.

Table 922 Configure the other querier timeout

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the other querier timeout	ip igmp query-timeout *seconds*	Optional By default, the other querier timeout is 255s.

Caution

- If the configure other querier timeout is smaller than the query interval, the querier in the network may change repeatedly.

Configure Fast Leave

The end segment in the network only connects to one host to perform the switching action of the multicast group frequently. To reduce the leave delay, you can configure the fast leave of the multicast group on the device.

After configuring the fast leave, the device receives the leave packet of one multicast group and checks whether the multicast group belongs to the fast leave range. If yes, the device does not send the specified group query packet to the segment any more and deletes the information of the multicast group immediately.

Table 923 Configure the fast leave

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the multicast group range of the fast leave	ip igmp immediate-leave group-list { *access-list-number* | *access-list-name* }	Mandatory By default, do not permit the fast leave of the multicast group, applicable to IGMPv2.
Configure the source group range of the fast leave	ip igmp sg-immediate-leave sg-list { *access-list-number* | *access-list-name* }	Mandatory By default, do not permit the fast leave of the source group, applicable to IGMPv3.

7.5.2.3 Configure IGMP SSM Mapping

Configuration Conditions

Before configuring the IGMP SSM mapping, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable;
- Enable the IGMP protocol.

Configure IGMP SSM Mapping

To provide the PIM-SSM service for the receiver not supporting IGMPv3 in the PIM-SSM network, we can configure the IGMP SSM Mapping function on the device.

The user can configure the IGMP SSM Mapping rule according to the demand of the network receiver. The group member relation report permitted by the rule is converted to the IGMPv3 non-member (IS_EX, TO_EX) relation report, and the multicast source address is the source address specified by the IGMP SSM mapping rule.

Table 924 Configure the IGMP SSM mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the IGMP SSM Mapping	ip igmp ssm-map enable [vrf *vrf-name*]	Mandatory By default, do not enable the IGMP SSM Mapping.
Configure the IGMP SSM Mapping rule	ip igmp ssm-map static { *access-list-number* | *access-list-name* } *source-ip-address* [vrf *vrf-name*]	Mandatory By default, there is no IGMP SSM Mapping rule.

Note

- The **ip igmp ssm-map static** command only supports the standard ACL.

7.5.2.4 IGMP Monitoring and Maintaining

Table 925 IGMP monitoring and maintaining

Command	Description
clear ip igmp group [*group-ip-address*] [*interface-name*] [vrf *vrf-name*]	Clear the IGMP multicast group information
clear ip igmp statistic interface *interface-name* [vrf *vrf-name*]	Clear the IGMP packet statistics information on the interface
show ip igmp groups [[static] | [*interface-name*] [*group-ip-address*] [detail]] [vrf *vrf-name*]	Display the IGMP multicast group information
show ip igmp interface [*interface-name*] [vrf *vrf-name*]	Display the interface IGMP information
show ip igmp statistic interface *interface-name* [vrf *vrf-name*]	Display the statistics information of the IGMP packets

7.5.3 IGMP Typical Configuration Example

7.5.3.1 Configure IGMP

Network Requirements

- The whole network runs the PIM-SM protocol.
- Device1, Device2, and Receiver are in the same LAN and Device2 is the querier.
- Receiver is one receiver of Device1 and Device2 end network.
- Run IGMPv2 between Device1, Device2 and end network.

Network Topology

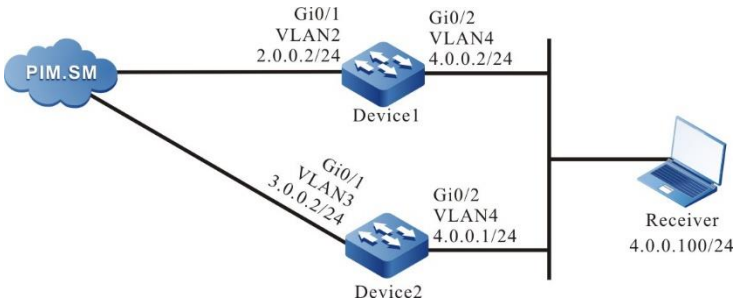


Figure 183 Networking of configuring IGMP

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

Step3: Check the result.

#View the IGMP version information and querier election result of Device1 interface vlan4.

```
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
```

#View the IGMP version information and querier election result of Device2 interface vlan4.

```
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 the IGMPv2 member relation report to add to multicast group 225.1.1.1.

#View the 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  V2 Expires
```

```
225.1.1.1       vlan4              00:21:02    00:03:47    4.0.0.100       stopped
```

#View the multicast member table of Device2.

```
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

- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run the IGMPv2 by default. You can configure the running IGMP version of the interface via the command ip igmp version.
- When multiple devices un IGMP in one LAN, elect the IGMP querier and the one with the smallest address is elected as the IGMP querier of the LAN.

7.5.3.2 Configure IGMP SSM Mapping

Network Requirements

- The whole network runs the PIM-SSM protocol.
- Receiver1, Receiver2, Receiver3, and Device2 are all in one LAN.
- Run IGMPv3 between Device2 and the stub network.
- Use the IGMP SSM mapping on Device2 so that Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

Network Topology

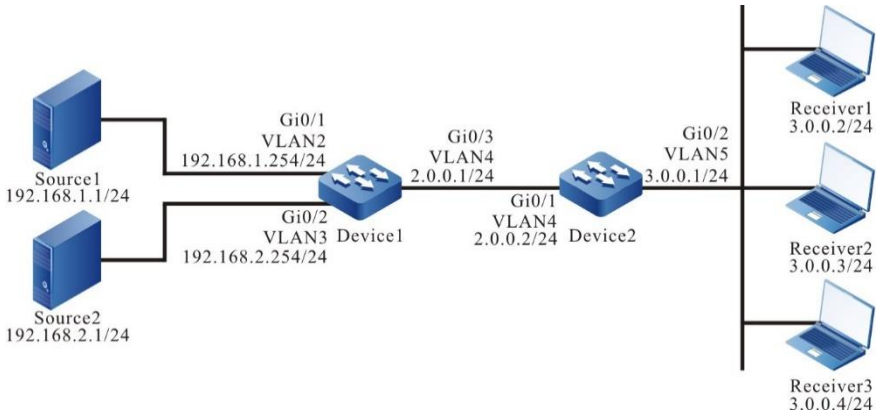


Figure 184 Networking of configuring the IGMP SSM mapping

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the unicast routing 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
```

#View the route 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

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.

Step 3: Enable the multicast forwarding globally, configure PIM-SSM globally and the multicast group range of the SSM service is 232.0.0.0/8. On the interfaces, enable the multicast protocol PIM-SM. The interface gigabitethernet1 of Device2 runs IGMPv3.

#Configure Device1.

Enable the multicast forwarding globally, configure the PIM-SSM globally and enable the multicast protocol PIM-SM on the interface.

```
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.

Enable the multicast forwarding globally, configure the PIM-SSM globally, and enable the multicast protocol PIM-SM on the interface. The interface gigabitethernet1 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
```

#View the IGMP information of the interface vlan5 on Device2.

```
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: Enable the IGMP SSM mapping on Device2 and configure the IGMP SSM mapping rule so that Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

#Configure Device2.

Enable the IGMP SSM mapping, configure the multicast group range of the IGMP SSM as 232.0.0.0~232.0.0.255, and the multicast source address is 192.168.1.1.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 232.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip igmp ssm-map enable
Device2(config)#ip igmp ssm-map static 1 192.168.1.1
```

#View the IGMP SSM mapping rule of Device2.

```
Device2#show ip igmp ssm-map

 IGMP SSM-MAP Information : enable
 acl-name   source-addr
 -------------------------
```

192.168.1.1

Step 5: Check the result.

Receiver1 sends the IGMPv3 member report packet of the specified source group to add to the multicast group 232.1.1.1 and the specified multicast source is 192.168.2.1; Receiver2 sends the IGMPv2 member report packet to add to the multicast group 232.1.1.2; Receiver3 sends the IGMPv1 member report packet to add to multicast group 232.1.1.3.

#Source1 and Source2 both send the multicast service packets with multicast groups 232.1.1.1, 232.1.1.2, and 232.1.1.3.

#View the multicast member table.

```
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
```

#View the PIM-SM multicast route table of Device2.

```
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 the multicast service packets sent by Source2; Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

Note

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.
- IGMP SSM mapping needs to be used with PIM-SSM; the multicast group range in the IGMP SSM mapping rule should belong to the PIM-SSM

multicast group range. IGMP SSM mapping mainly runs IGMPv1 or IGMPv2 and cannot be upgraded to the receiver host of IGMPv3 to provide the supporting for the SSM model.

- The IGMP SSM mapping is invalid for the IGMPv3 member report packet.

7.5.3.3 Configure IGMP Static Adding

Network Requirement

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of the Device end network.
- Run IGMPv2 between Device and the end network.
- Device interface vlan3 adds to multicast group 225.1.1.1 statically.

Network Topology

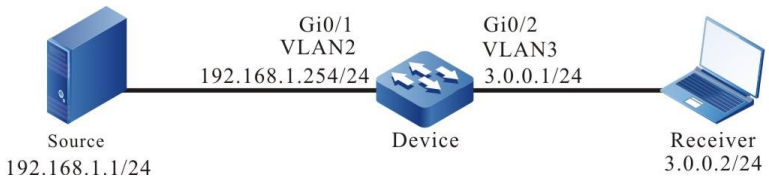


Figure 185 Networking of configuring IGMP static adding

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

#View the IGMP information of Device interface vlan3.

```
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 interface vlan3 adds to multicast group 225.1.1.1 statically.

#Configure Device.

Device interface vlan3 adds to multicast group 225.1.1.1 statically.

```
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 the multicast packet with multicast group 225.1.1.1.

#View the multicast member table of Device.

```
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
```

#View the multicast route table of Device.

```
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 packet with multicast group 225.1.1.1 sent by Source.

7.5.3.4 Configure IGMP Multicast Group Filter

Network Requirement

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of the Device end network.
- Run IGMPv2 between Device and the end network.
- Device interface vlan3 filters the multicast group; the range of the multicast groups Receiver is permitted to add is 225.1.1.0-225.1.1.255.

Network Topology

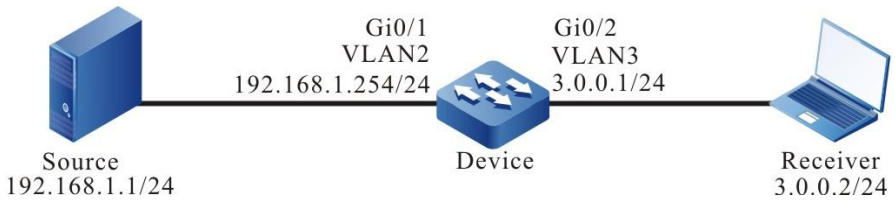


Figure 186 Networking of configuring IGMP multicast group filter

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

#View the IGMP information of Device interface vlan3.

```
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 the multicast group filter on Device interface vlan3.

#Configure Device.

Configure the multicast group filter on Device interface vlan3; the range of the multicast groups Receiver is permitted to add 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)#commit
Device(config-std-nacl)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ip igmp access-group 1
Device(config-if-vlan3)#exit
```

Step4: Check the result.

#Receiver sends the IGMPv2 member relation report to add to multicast group 225.1.1.1 and 226.1.1.1.

#Source sends the multicast packets with multicast group 225.1.1.1 and 226.1.1.1.

#View the multicast member table of Device.

```
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
```

#View the multicast route table of Device.

```
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 service packets with multicast group 225.1.1.1 sent by Source.

Note

- To filter based on multicast source group, use the command ip igmp ssm-access-group to realize. When using the command, it is required that the device runs PIM-SSM and the interface runs IGMPv3.

7.6 PIM-DM

7.6.1 Overview

PIM-DM (Protocol Independent Multicast-Dense Mode) is applicable when the group members are relatively concentrated and the range is small, or the network bandwidth resource is sufficient.

PIM-DM does not depend on the specified unicast route protocol for the RPF check.

PIM-DM adopts the “Push” to transmit the multicast packets. When the multicast source starts to send the multicast packets, suppose that all subnets in the multicast domain have the multicast receivers, so the multicast packets are pushed to all nodes in the network. PIM-DM forwards and prunes the multicast without the receiver. When the node of the pruned multicast forwarding branch node has the receiver of the multicast source, PIM-DM uses the graft mechanism to actively restore the forwarding of the multicast data.

PIM-DM uses the status refresh mechanism to refresh the downstream status regularly so that the pruned branch does not time out.

7.6.2 PIM-DM Function Configuration

Table 926 PIM-DM function configuration list

Configuration Task	
Configure PIM-DM basic functions	Configure the PIM-DM protocol
Configure the PIM-DM neighbor	Configure the period of sending the HELLO packets
	Configure PIM-DM neighbor keepalive time
	Configure PIM-DM neighbor filter
Configure the status refresh parameters	Configure PIM-DM status refresh interval

Caution

- The L3 Ethernet interface does not support the PIM-DM function.

7.6.2.1 Configure PIM-DM Basic Functions

Configuration Condition

Before configuring PIM-DM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing the intra-domain route reachable
- Enable IP multicast forwarding function

Configure PIM-DM Protocol

Table 927 Configure the PIM-DM protocol

Step	Command	Description
Enter global configuration	configure terminal	-

Step	Command	Description
mode		
Enter interface configuration mode	interface *interface-name*	-
Enable the PIM-DM protocol.	ip pim dense-mode ip pim dense-mode passive	Either By default, PIM-DM is disabled on the interface. Enable the PIM-DM protocol via ip pim dense-mode passive. The interface does not send the hello packets to the neighbor.

7.6.2.2 Configure PIM-DM Neighbor

Configuration Condition

Before configuring the PIM-DM neighbor, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing intra-domain route reachable
- Enable the PIM-DM protocol

Configure Sending Period of HELLO Packets

The interface enabled with the PIM-DM protocol periodically sends the Hello packets to set up and maintain the PIM-DM neighbor.

Table 928 Configure the period of sending HELLO packets

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the period of	ip pim dense-mode hello-interval *interval-value*	Optional

Step	Command	Description
sending the Hello packets		By default, the period of sending the Hello packets is 30s.

Configure PIM-DM Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 929 Configure PIM-DM neighbor keepalive time

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the keepalive time of the PIM-DM neighbor	ip pim dense-mode hello-holdtime *holdtime-value*	Optional By default, the keepalive time of the PIM-DM neighbor is 105s.

Configure PIM-DM Neighbor Filter

To save the system resources, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 930Configure the PIM-DM neighbor filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface	interface *interface-name*	-

Step	Command	Description
configuration mode		
Configure the PIM-DM neighbor filter	ip pim dense-mode neighbor-filter {access-*list-number* | *access-list-name* }	Optional By default, do not enable the PIM-DM neighbor filter function.

7.6.2.3 Configure Status Refresh Parameters

Configuration Condition

Before configuring the PIM-DM status refresh parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing intra-domain route reachable
- Enable the PIM-DM protocol

Configure PIM-DM Status Refresh Interval

PIM-DM needs to set the interval of the router directly-connected to the source generating the status refresh packets

Table 931 Configure the PIM-DM status refresh interval

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the PIM-DM status refresh interval	ip pim dense-mode state-refresh origination-interval *interval-value*	Optional By default, the PIM-DM status refresh interval is 60s.

7.6.2.4 PIM-DM Monitoring and Maintaining

Table 932 PIM-DM monitoring and maintaining

Command	Description
clear ip pim dense-mode mroute [*group-ip-address source-ip-address*] [vrf *vrf-name*]	Clear the PIM-DM multicast route information
show ip pim dense-mode interface [detail] [vrf *vrf-name*]	Display the PIM-DM interface information
show ip pim dense-mode neighbor [detail] [vrf *vrf-name*]	Display the PIM-DM neighbor information
show ip pim dense-mode nexthop [*source-ip-address*] [vrf *vrf-name*]	Display the unicast next-hop information from PIM-DM to source
show ip pim dense-mode mroute [[group *group-ip-address* [source *source-ip-address*]]| [source *source-ip-address* group *group-ip-address*]] [vrf *vrf-name*]	Display the route table information of the PIM-DM protocol

7.6.3 PIM-DM Typical Configuration Example

7.6.3.1 Configure PIM-DM Basic Functions

Network Requirements

- The whole network enables the PIM-DM protocol.
- Receiver is one receiver of the Device2 end network.
- Run IGMPv2 between Device2 and the end network.

Network Topology

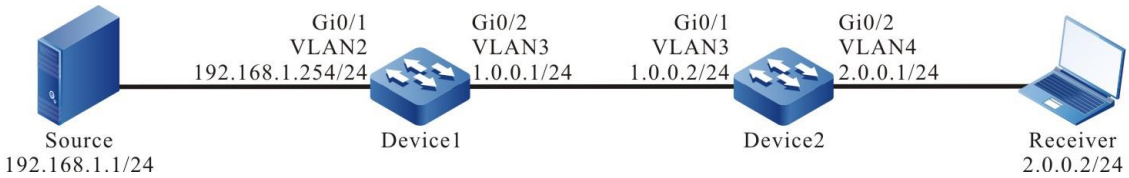


Figure 187 Networking of configuring the PIM-DM basic functions

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: Enable the unicast route 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 1.0.0.0 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 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#View the route 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, 00:07:30, vlan3
C   2.0.0.0/24 is directly connected, 00:07:14, vlan4
O   192.168.1.0/24 [110/2] via 1.0.0.1, 00:00:16, vlan3
```

Note

- The method of viewing the route table of Device1 is the same as that of Device2.

Step 4: Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

```
Device1(config)#ip multicast-routing
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ip pim dense-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ip pim dense-mode
Device1(config-if-vlan3)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

```
Device2(config)#ip multicast-routing
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip pim dense-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ip pim dense-mode
Device2(config-if-vlan4)#exit
```

#View the information of the interface enabled with the PIM-DM protocol on Device2 and the PIM-DM neighbor information.

```
Device2#show ip pim dense-mode interface
Total 2 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
Address         Interface         VIFIndex Ver/    Nbr    VIF
                                           Mode    Count  Flag
1.0.0.2         vlan3             0        v2/D    1      UP
2.0.0.1         vlan4             1        v2/D    0      UP
Device2#show ip pim dense-mode neighbor
PIM Dense-mode Neighbor Table:
PIM Dense-mode VRF Name: Default
Total 1 Neighbor entries
```

```
Neighbor-Address Interface        Uptime/Expires    Ver
1.0.0.1          vlan3            00:02:15/00:01:30 v2
```

#View the IGMP information of interface VLAN4 of Device2.

```
Device2#show ip igmp interface vlan 4
Interface vlan4 (Index 65547)
 IGMP Active, Querier (2.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 2.0.0.1
 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 method of viewing the Device1 information is the same as that of Device2.
- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run IGMPv2 by default. You can configure the running IGMP version on the interface by executing the ip igmp version command.

Step5: Check the result.

#Receiver sends the IGMPv2 member relation report to add to multicast group 225.1.1.1.

#Source sends the multicast packets with multicast group 225.1.1.1.

#View the multicast member table of Device2.

```
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            00:06:01 00:04:06 2.0.0.2         stopped
```

#View the PIM-DM multicast route table of Device2.

```
Device2#show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
Total 1 mroute entries
(192.168.1.1, 225.1.1.1)
  Expire in: 00:02:35
  RPF Neighbor: 1.0.0.1, Nexthop: 1.0.0.1, vlan3
  Upstream IF: vlan3
    Upstream State: Forwarding
    Assert State: Loser
  Downstream IF List:
    vlan4, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

#Receiver can receive the multicast packets with the multicast group 225.1.1.1 sent by Source.

Note

- The method of viewing the Device1 information is the same as that of Device2.

7.7 PIM-SM

7.7.1 Overview

PIM-SM (Protocol Independent Multicast, Sparse Mode) is applicable when the group members are relatively dispersive and their range is relatively broad or the network bandwidth resource is relatively limited.

PIM-SM does not depend on any particular unicast route protocol. The device announces the multicast information to all PIM-SM routers by actively sending the

packets to request to set up multicast distributing tree (MDT) and set RP (Rendezvous Point) and BSR (Bootstrap Router). When the receiver adds to one multicast group, the receiving end DR (Designated Router) sends the PIM adding packet to RP, constructing the sharing tree-RPT with RP as root, while the source DR registers the multicast source to RP, constructing the source tree with the multicast source as root. The multicast service packets are transmitted to the receiver along the source tree and sharing tree; the receiving end DR sends the PIM adding packet to the multicast source. At last, switch from RPT to source-based SPT (Shortest-path Tree), so as to reduce the network delay.

PIM SSM is short for Protocol Independent Multicast ---- Source Specific Multicast. PIM-SSM is the subset of the PIM-SM protocol and should run on the basis of PIM-SM. The PIM-SSM protocol set the IPv4 address 232.0.0.0-232.255.255.255 to be reserved for SSM. PIM-SSM should work with IGMPv3, because IGMPv3 can send the IGMP membership report packet of the specified source and group.

7.7.2 PIM-SM Function Configuration

Table 933 PIM-SM function configuration list

Configuration Task	
Configure the PIM-SM basic functions	Enable the PIM-SM protocol
Configure the PIM-SM aggregation router	Configure C-RP
	Configure static RP
Configure the PIM-SM bootstrap router	Configure C-BSR
	Configure the BSR edge
Configure PIM-SM multicast source registration	Configure the RP reachability check
	Configure the sending rate of the register packets
	Configure sending rate of the register stop packets
	Configure the source address of the register packet
	Configure register packet filter

Configuration Task	
Configure PIM-SM neighbor parameters	Configure the period of sending the Hello packets
	Configure the keepalive time of the neighbor
	Configure the neighbor filter
	Configure the DR priority
Configure PIM-SM SPT switching	Configure the SPT switching condition
Configure PIM-SSM	Configure PIM-SSM
Configure PIM-SDM	Enable PIM-SDM

Caution

- L3 Ethernet interface does not support the PIM-SM function.

7.7.2.1 Configure PIM-SM Basic Functions

Configuration Condition

Before configuring PIM-SM, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable

Enable PIM-SM Protocol

Table 934 Enable the PIM-SM protocol

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the IP multicast forwarding	ip multicast-routing	Mandatory By default, the IP multicast

Step	Command	Description
		forwarding is not enabled.
Enter interface configuration mode	interface *interface-name*	-
Enable the PIM-SM protocol	ip pim sparse-mode	Either By default, PIM-SM is disabled on the interface.
	ip pim sparse-mode passive	

Note

- After enabling the PIM-SM protocol, automatically enable the IGMP protocol.
- After enabling the PIM-SM function, all PIM-SM configurations can take effect.

7.7.2.2 Configure PIM-SM Aggregation Router

Configuration Condition

Before configuring RP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Configure C-RP

RP is generated by the C-RO election. After BSR is elected, all C-RPs (Candidate-Rendezvous Point) regularly send the unicast C-RP packet to BSR. BSR integrates the C-RP information and transmits the information to all devices in the PIM-SM domain via the bootstrap packet.

Table 935 Configure C-RP

Step	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*]	Mandatory By default, there is no C-RP.

Note

- RP election rules:
- For the group range of the C-RP service, perform the longest matching of the mask.
- If the longest matching of the mask has multiple C-RPs, compare the C-RP priority. The smaller the value, the high the priority. The one with highest priority wins.
- If there are multiple C-RPs with highest priority, perform the HASH calculation for the C-RP address and group. The one with the largest HASH value wins.
- If there are multiple RPs with the largest HASH, the C-RP with the largest IP address wins.

Configure Static RP

For the simple PIM-SM network, it is suggested to use the static RP. If using the static RP, do not need to perform the BSR configuration, eliminating the frequent interacting between RP and BSR, so as to save the network bandwidth.

Table 936 Configure static RP

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the static RP	ip pim rp-addressess *ip-address* [*access-list-name* | *access-list-number*] [override] [vrf *vrf-name*]	Mandatory By default, there is no static RP.

Note

- All devices in the same PIM-SM domain should be configured with the same static RP.

7.7.2.3 Configure PIM-SM Bootstrap Router

Configuration Condition

Before configuring BSR, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Configure C-BSR

In one PIM-SM domain, there should be the unique BSR. Multiple C-BSRs (Candidate-Bootstrap Router) elects to generate the unique BSR via the bootstrap packet.

Table 937 Configure C-BSR

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure C-BSR	ip pim bsr-candidate *interface_name* [*hash-mask-length* [*priority-value*]] [vrf *vrf-name*]	Mandatory By default, there is no C-BSR.

Note

- BSR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IP address wins.

Configure BSR Border

BSR is responsible for collecting the C-RP information and transmits the information to all devices in the PIM-SM domain via the bootstrap packet. The BSR range is the range of the multicast domain. The bootstrap packet cannot pass the interface configured with the BSR border. The devices out of the multicast domain range cannot take part in the forwarding of the multicast service packet in the multicast domain, so as to realize the dividing of the multicast domain.

Table 938 Configure the BSR border

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the BSR border	ip pim bsr-border	Mandatory By default, there is no multicast border.

7.7.2.4 Configure PIM-SM Multicast Source Register

Configuration Condition

Before configuring the multicast source register, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Configure RP Reachability Check

Before source DR sends the register packet to RP, first perform the RP reachability check. If finding that the RP route is not reachable, do not register to RP, so as to reduce the cost of the DR.

Table 939 Configure the RP reachability check

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the RP reachability check	ip pim register-rp-reachability [vrf *vrf-name*]	Mandatory By default, before performing the PIM register, do not check the RP reachability.

Note

- To reduce the cost of the source DR, it is suggested to configure the command on the source DRs of all PIM-SMs.

Configure Sending Rate of Register Packets

When the source DR receives the multicast packet, encapsulate the multicast

packet to the register packet and send to RP for source register until the registration is complete..

When the source DR does not complete the multicast source register and the multicast flow is large, generate lots of register packets, which increase the load of the RP device. Even RP cannot work normally. Source DR does not need to transmit all register packets of one flow to RP, so configuring the rate of sending the register packets at the source DR not only can reach the purpose of source registration, but also can reduce the RP load.

Table 940 Configure the rate of sending the register packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the rate of sending the register packet	ip pim register-rate-limit *rate-limit-value* [vrf *vrf-name*]	Mandatory By default, do not limit the rate of sending the register packet.

Note

- To reduce the RP load, it is suggested to configure the rate of sending the source register packets on all source DRs.

Configure Sending Rate of Register Stop Packets

After RP receives the register packet of the source DR, send the register stop packet to the source DR to complete the registration. When the RP receives lots of register packets, it is necessary to reply all register packets (send register stop packet). In fact, there are lots of repeated packets in the register stop packets. You can limit the rate of sending the register stop packet on RP to reduce the cost of RP.

Table 941 Configure the rate of sending the register stop packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the rate of sending the register stop packet	ip pim register-stop-rate-limit *rate-limit-value* [vrf *vrf-name*]	Mandatory By default, do not limit the rate of sending the register stop packet.

Note

- To improve the robustness of the whole PIM-SM network, it is suggested to limit the rate of the source register stop packet on all RPs.

Configure Source Address of Register Packet

When the source DR performs the source register, the source address of the register packet uses the IP address of the register interface automatically registered by the system. The command can specify the source address of the register packet as the IP address of one interface on the device to meet some special demand of the network.

Table 942 Configure the source address of the register packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the source address of the register packet	ip pim register-source interface *interface-name* [vrf *vrf-name*]	Mandatory By default, use IP address of the register interface automatically registered by the system as the source address of the register packet.

Configure Register Packet Filter

To prevent the source register attack, you can use ACL on RP to perform the multicast source filter for the register packet. Only the multicast source permitted by ACL can register successfully on RP.

Table 943 Configure the register packet filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the register packet filter	ip pim accept-register list { *access-list-number* | *acees-list-name* } [vrf *vrf-name*]	Mandatory By default, do not filter the register packet.

7.7.2.5 Configure PIM-SM Neighbor Parameters

Configuration Condition

Before configuring the PIM-SM neighbor parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Configure Sending Period of Hello Packets

The interface enabled with the PIM protocol periodically sends the Hello packets to set up and maintain the PIM neighbor.

Table 944 Configure the period of sending the Hello packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the period of sending the Hello packet	ip pim hello-interval *interval-value*	Optional By default, the period of sending the Hello packet is 30s.

Configure Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 945 Configure PIM-SM neighbor keepalive time

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure PIM-SM neighbor keepalive time	ip pim hello-holdtime *holdtime-value*	Optional By default, the keepalive time of the PIM-SM neighbor is 105s.

Configure Neighbor Filter

If there are many PIM neighbors in one subnet, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 946 Configure the neighbor filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the neighbor filter	ip pim neighbor-filter { *access-list-number* | *acees-list-name* }	Mandatory By default, do not enable the neighbor filter function.

Configure DR Priority

DR plays one important role in the PIM-SM network, so selecting the appropriate DR is important. You can select the appropriate device as DR by configuring the DR priority.

One PIM-SM subnet only permits one DR. According to the function, DR can be divided to source DR and receiving DR.

The main function of the source DR is to perform the source register to RP.

The main function of the receiving DR is to add to RP and set up the switching of RPT and SPT.

Table 947 Configure the DR priority

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the DR priority	ip pim dr-priority *priority-value*	Optional By default, the DR priority is 1.

Note

- DR election rules:

- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IP address wins.

7.7.2.6 Configure PIM-SM SPT Switching

Configuration Condition

Before configuring SPT, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Configure SPT Switching Condition

The receiving end DR does not know the address of the multicast source, so it can only add to RP to form RPT. The source DR performs the source register to RP and form the source tree between source DR and RP. At first, the direction of the multicast flow is from multicast source to RP and then from RP to the receiver. When the receiving end DR receives the first multicast packet, it performs adding to multicast source, forms SPT, and performs the pruning for RPT. This is called SPT switching.

The command is to configure the SPT switching condition at the receiving end DR.

Table 948 Configure the SPT switching condition

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the SPT	ip pim spt-threshold infinity [group-list	Mandatory

Step	Command	Description
switching condition	{ *access-list-number* | *acees-list-name* }] [vrf *vrf-name*]	By default, all multicast groups perform the SPT switching.

Caution

- Do not configure SPT never-switching on RP. Otherwise, it may result in the failure of the multicast forwarding.

7.7.2.7 Configure PIM-SSM

PIM-SSM is one subset of PIM-SM. In PIM-SSM, do not need RP, BSR or RPT, and there is no SPT switching, but the receiving end DR directly adds to multicast source and sets up the shortest path tree (SPT) with source as root.

Configuration Condition

Before configuring PIM-SSM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol on all interfaces that need multicast route forwarding

Configure PIM-SSM

Table 949 Configure PIM-SSM

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure PIM-SSM	ip pim ssm { default | range { *access-list-number* | *acees-list-name* } } [vrf *vrf-name*]	Mandatory By default, the SSM function is disabled.

Caution

- When using PIM-SSM, the receiving end should enable IGMPv3.
- When the receiver cannot be upgraded to IGMPv3, you can use the IGMP SSM Mapping function to cooperate with PIM-SSM.
- Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent. Otherwise, it may result in the abnormality of PIM-SS.

7.7.2.8 Configure PIM Adaptive Basic Functions

Configuration Condition

Before configuring PIM-SDM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable

Configure PIM Adaptive Basic Functions

Table 950 Configure PIM-SDM

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the IP multicast forwarding	ip multicast-routing [vrf *vrf-name*]	Mandatory By default, do not

Step	Command	Description
		enable the IP multicast forwarding.
Enter the interface configuration mode	interface *interface-name*	-
Configure the PIM adaptive function	ip pim sparse-dense-mode	Either By default, the PIM adaptive function is disabled.
	ip pim sparse-dense-mode passive	

Note

- After the PIM adaptive function is enabled on the interface, PIM-SM, PIM-DM, and IGMP protocols will be enabled automatically.

7.7.2.9 Configure PIM-SM Control Policy

Configure Interface Concerned DR Status Change

Non-DR enables L2 multicast forwarding, and stops the L3 multicast forwarding. DR is not affected.

Table 951 Configure the DR priority

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the interface to concern DR status change	ip pim drchg-attention	By default, it is L3 multicast forwarding.

Configure the Interface to Suppress PIM-JOIN Packet

Table 952 Configure the interface to suppress the PIM-JOIN packet.

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the interface to suppress the PIM-JOIN packet.	ip pim join-suppression	By default, do not suppress the interface PIM-JOIN packet.

7.7.2.10 Configure PIM-SM to Support (*,*,rp)

Configuration Conditions

Before configuring PIM-SM to support (*,*,rp), first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the PIM-SM protocol

Enable Supporting (*, *,rp)

Table 953 Enable PIM-SM to support (*,*,rp)

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable PIM-SM to support (*,*,rp)	ip pim mbr [vrf *vrf-name*]	Mandatory By default, do not PIM-SM to support (*,*,rp).

7.7.2.11 Configure PIM-SM BFD

Configuration Conditions

Before configuring PIM-SM BFD, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable

Configure PIM-SM BFD

Table 954 Configure PIM-SM BFD

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure PIM-SM BFD	ip pim bfd	By default, do not enable the PIM-SM BFD function.

7.7.2.12 PIM-SM Monitoring and Maintaining

Table 955 PIM-SM monitoring and maintaining

Command	Description
clear ip pim bsr rp-set [vrf *vrf-name*]	Clear the RP set information of PIM-SM
clear ip pim mroute [*group-address* [*source-address*]] [vrf *vrf-name*]	Clear the multicast route information of PIM-SM
clear ip pim statistics [interface *interface-name* | vrf *vrf-name*]	Clear the statics information of the PIM-SM protocol packets
show ip pim bsr-router [vrf *vrf-name*]	Display the PIM-SM bootstrap route information
show ip pim interface [[*interface-name*] detail] [vrf *vrf-name*]	Display the PIM-SM interface information
show ip pim local-members [*interface-name* | vrf *vrf-name*]	Display the PIM-SM local group member information

Command	Description
show ip pim mroute [ssm | group *group-ip-address* [source *source-ip-address*] | source *source-ip-address*] [vrf *vrf-name*]	Display the PIM-SM multicast route table information
show ip pim neighbor [detail] [vrf *vrf-name*]	Display the PIM-SM neighbor information
show ip pim nexthop [*ip-address*] [vrf *vrf-name*]	Display the PIM-SM next-hop router information
show ip pim rp mapping [vrf *vrf-name*]	Display the PIM-SM RP information
show ip pim rp-hash *group-address* [vrf *vrf-name*]	Display the RP information of the multicast group mapping
show ip pim statistics [vrf *vrf-name*]	Display the statistics information of the PIM-SM protocol packets

7.7.3 PIM-SM Typical Configuration Example

7.7.3.1 Configure PIM-SM Basic Functions

Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver1 and Receiver2 are the two receivers of Device3 end network.
- Device1 and Device2 are C-BSR and C-RP.
- Run IGMPv2 between Device3 and the end network.

Network Topology

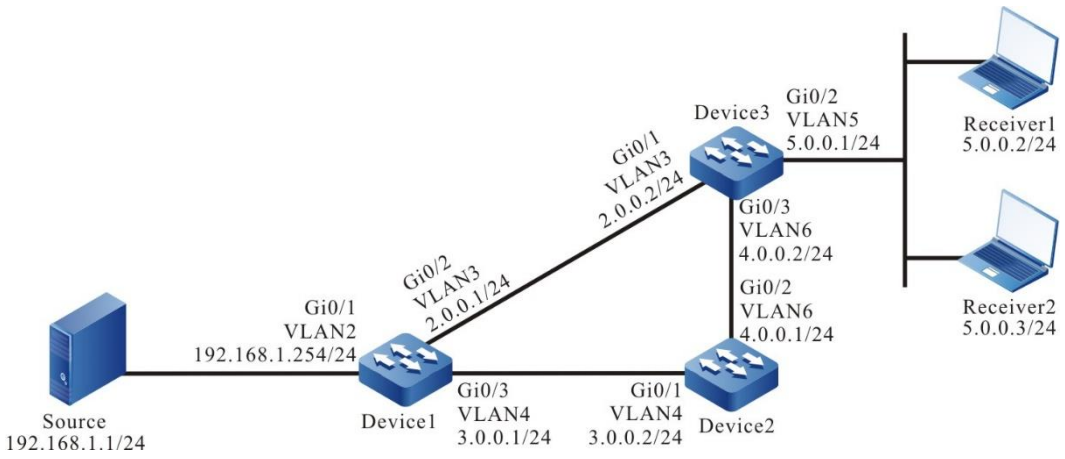


Figure 188 Networking of configuring PIM-SM basic functions

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the unicast route 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
```

#View the route 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

#View the IGMP information of interface VLAN5 of 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
```

Caution

- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run IGMPv2 by default. You can configure the running IGMP version on the interface by **executing the ip igmp version** command.

Step 4: Configure interface vlan3 of Device1 as C-BSR and C-RP; configure the interface vlan4 of Device2 as C-BSR and C-RP.

#Configure Device1.

Configure interface vlan3 of Device1 as C-BSR and C-RP; the priority of C-BSR is 200; the multicast group range of the C-RP service is 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)#commit
Device1(config-std-nacl)#exit
Device1(config)#ip pim rp-candidate vlan 3 group-list 1
```

#Configure Device2.

Configure interface vlan4 of Device2 as C-BSR and C-RP; the priority of C-BSR is 0; the multicast group range of the C-RP service of Device2 is 230.0.0.0/4.

```
Device2(config)#ip pim bsr-candidate vlan4
Device2(config)#ip pim rp-candidate vlan4
```

#View the BSR and RP information of Device3.

```
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
```

Caution

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- When configuring multiple C-BSRs in one multicast domain, first elect BSR according to the priority and the C-BSR with the largest priority is elected as BSR. When the priorities of C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR.
- When configuring multiple C-RPs in one multicast domain and the service multicast group ranges are the same, calculate the RP of the multicast group G according to the hash algorithm.
- In the multicast domain, you can configure RP via the command ip **pim rp-address**, but it is required that the static RP addresses configured on all devices in the multicast domain keep consistent.

Step 5: Check the result.

Receiver1 and Receiver2 send the IGMPv2 member relation reports to add to multicast group 225.1.1.1, 230.1.1.1 respectively.

#Source sends the multicast packets with multicast group 225.1.1.1, 230.1.1.1.

#View the multicast member table of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 2 groups
Group Address   Interface         Uptime   Expires  Last Reporter   V1 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
```

#View the RP of multicast group 225.1.1.1,230.1.1.1 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
```

#View the multicast route 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 service packet with multicast group 225.1.1.1 sent by Source. Receiver2 can only receive the multicast service packet with multicast group 230.1.1.1 sent by Source.

Note

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.
- By default, the device enables the SPT switching.

7.7.3.2 Configure PIM-SSM

Network Requirements

- The whole network runs the PIM-SSM protocol.
- Receiver is one receiver of Device3 end network.
- Run IGMPv3 between Device3 and the end network.

Network Topology

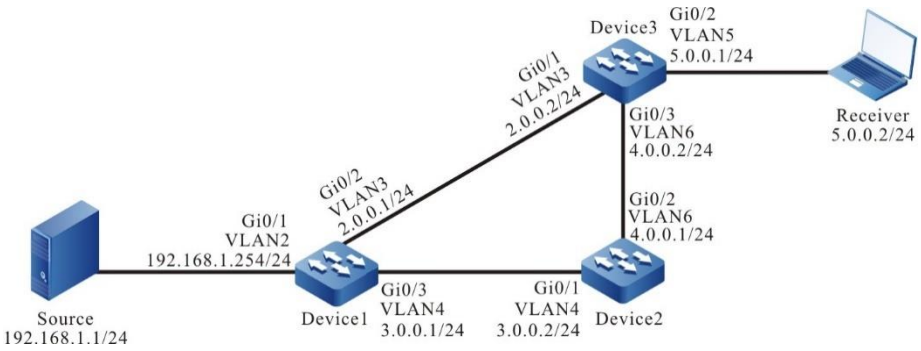


Figure 189 Networking of configuring PIM-SSM

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the unicast route 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
```

#View the route 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 4: Configure PIM-SSM on all devices; the multicast group range of the SSM service is 232.0.0.0/8. vlan5 of Device3 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
```

#View the IGMP information of interface VLAN5 of 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 the IMGPv3 member relation report of the specified source group to add to multicast group 232.1.1.1; the specified multicast source is 192.168.1.1

#Source sends the multicast packets with multicast group 232.1.1.1.

#View the multicast member table 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
```

#View the multicast route 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 service packet with multicast group 232.1.1.1 sent by Source.

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- The default multicast group range of PIM-SSM is 232.0.0.0/8. You can modify the multicast group range of the 232.0.0.0/8 service via the command ip pim ssm range.
- For the multicast group G meeting the SSM condition, the multicast route table does not generate the (*,G) entry, but just generate the (S,G) entry.

7.7.3.3 Configure PIM-SM Multicast Forwarding Control

Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of Device3 end network.
- Device2 is C-BSR and C-RP.
- On Device2 and Device3, control the multicast source, making Receiver only receive the multicast service packet sent by Source1.
- Run IGMPv2 between Device3 and the end network.

Network Topology

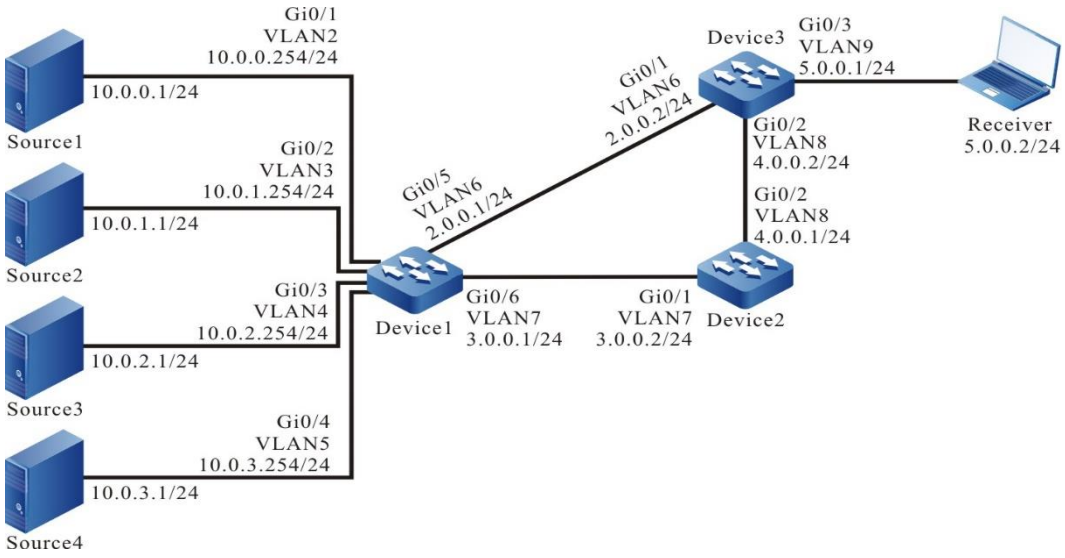


Figure 190 Networking of configuring PIM-SM multicast forwarding control

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the unicast route 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
```

#View the route 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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 the multicast forwarding and enable the multicast protocol PIM-SM on the related 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
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 4: Configure vlan7 of Device2 as C-BSR and C-RP of the whole network and the multicast group range of the C-RP service is 224.0.0.0/4.

#Configure Device2.

```
Device2(config)#ip pim bsr-candidate vlan7
Device2(config)#ip pim rp-candidate vlan7
```

#View the BSR and RP information of Device3.

```
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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 5: On Device2 and Device3, control for the multicast source, making Receiver only receive the multicast service packet sent by Source1

#On Device2, configure the accepted register message access list, filtering the register message of Source4.

```
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)#commit
Device2(config-std-nacl)#exit
Device2(config)#ip pim accept-register list 1
```

#On interface vlan6 and vlan8 of Device3, configure the ingress ACL, filtering

the multicast service packets of Source3.

```
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
Device2(config-std-nacl)#commit
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 interface vlan9 of Device3, configure the ingress ACL, filtering the multicast service packets of Source2.

```
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)#commit
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 the IMGPv2 member relation report to add to multicast group 225.1.1.1.

Source1, Source2, Source3, and Source4 send the multicast packets with multicast group 225.1.1.1.

#View the multicast member table of Device2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
```

```
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1        vlan9 00:00:38 00:03:45 5.0.0.2          stopped
```

#View the multicast route 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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

#View the matching of ACL on Device2.

```
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
```

#View the matching of ACL on Device3.

```
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 end can only receive the multicast service packets sent by Source1.

Caution

- When performing the multicast source control, you'd better first configure the multicast source control and then on-demand multicast source, because by default, after receiving the multicast service packet, the receiving end DR performs the SPT switching. If first on-demanding multicast source and then performing the multicast forwarding control, the multicast forwarding control does not take function. To prevent the multicast forwarding control

from not taking function, you can configure not permitting SPT switching on the receiving end DR.

7.7.3.4 Configure DR Switching Convergence of PIM-SM and BFD Linkage

Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of Device3 end network.
- Device2 and device3 are located in the stub network of the receiver, and device3 is the receiver DR.
- The line between device2 and device3 enables PIM BFD. When the line between device3 and receiver fails, Device2 will quickly switch to receiver DR.

Network Topology

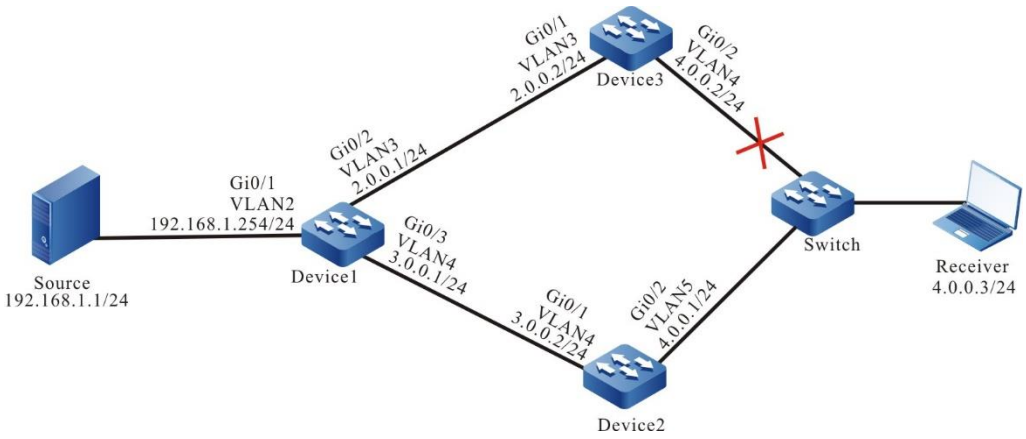


Figure 191 Networking of configuring the DR switching convergence of PIM-SM and BFD linkage

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the 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 route 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
```

Caution

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable multicast forwarding, and enable multicast protocol PIM-SM on the interface.

#Configure Device1.

Enable multicast forwarding globally and enable multicast protocol PIM-SM on related 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.

Enable multicast forwarding globally and enable multicast protocol PIM-SM on related 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.

Enable multicast forwarding globally and enable multicast protocol PIM-SM on related 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
```

#View the information of the interface on Device 3 enabled with the PIM-SM

protocol and the neighbor information of PIM-SM.

```
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 /
```

#You can see that Device3 is the receiver DR of the stub network where Receiver is located.

Caution

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 4: Configure C-BSR and C-RP.

#Configure Device1.

Configure VLAN2 of Device1 as C-BSR and C-RP of the whole network, and the multicast group range of C-RP service is 224.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate vlan 2
```

```
Device1(config)#ip pim rp-candidate vlan 2
```

#View the BSR and RP information of Device3.

```
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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 5: On Device2 and Device3, configure PIM and BFD linkage.

#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
```

#Query the BFD session information of Device3.

```
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
```

#You can see that PIM is associated with BFD successfully.

Note

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

Step 6: Check the result.

#Receiver sends the IGMPv2 membership report to join the multicast group 225.1.1.1, and Source sends the multicast service packet with the multicast group 225.1.1.1.

#View the multicast member tables on Device2 and Device3.

```
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
```

#View the PIM-SM multicast route tables on Device2 and Device3.

```
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 that the upstream state of PIM-SM multicast routing table of Device2 is NOT JOINED, the upstream state of Device3 multicast route is JOINED, and multicast service packets are forwarded to Receiver through Device3.

#When the line between Device3 and Receiver fails, BFD will quickly detect and notify PIM-SM protocol, and Device2 will quickly switch to receiver Dr.

#View the PIM-SM neighbor information, BFD session information and PIM-SM multicast route table of Device2.

```
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:
```

#View the PIM-SM neighbor, BFD session, and multicast route table of Device3.

```
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 after the receiver DR Device3 fails, the BFD session responds immediately, and Device2 switches to the receiver DR. the multicast service packet is forwarded to Receiver through Device2.

Note

- BFD and PIM linkage is also applicable to the scenario of Asset campaign on shared network segment. When the interface of Assert Winner fails, Assert Loser can respond quickly and recover forwarding multicast packets.

7.7.3.5 Configure RPF Route Switching Convergence of PIM-SM and BFD Linkage

Network Requirements

- The whole network runs the PIM-SM protocol.
- Device2 is C-BSR and C-RP.
- The whole network uses OSPF to interact the unicast route.
- The PIM BFD and OSPF BFD detection functions are enabled for the line between Device1 and Device3. After the line fails, the BFD can quickly detect and notify the PIM and OSPF protocols, so that the RPF neighbor from Device3 to the multicast source can quickly switch to Device2.

Network Topology

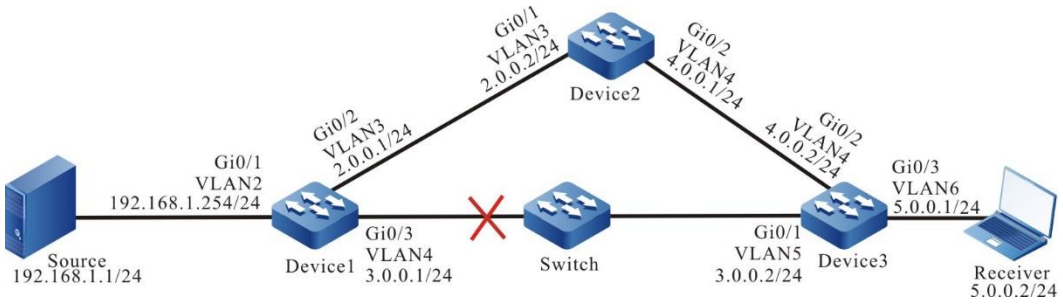


Figure 192 Networking of configuring RPF route switching of PIM-SM and BFD linkage

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable unicast routing protocol, 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
```

#Query the unicast route 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   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

- The viewing methods of Device1 and Device2 are the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable multicast forwarding, and enable multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable multicast forwarding and enable multicast protocol PIM-SM on the related 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 the related 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 the related 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
```

#Query the information of the interface on Device3 enabled with the PIM-SM protocol and the PIM-SM neighbor 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 VLAN3 of Device2 C-BSR and C-RP of the whole network, and the multicast group range of C-RP service is 224.0.0.0/8.

```
Device2(config)#ip pim bsr-candidate vlan 3
Device2(config)#ip pim rp-candidate vlan 3
```

#Query the BSR and RP information of Device3.

```
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: Configure PIM, OSPF to link with BFD on Device1 and Device3.

#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
```

#Query the BFD session information of Device3.

```
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
```

#You can see that the BFD session between Device1 and Device3 is established normally, and OSPF and PIM protocols are successfully associated.

Note

- The viewing methods of Device1 are the same as that of Device3, so the viewing process is omitted.

Step 6: Check the result.

#Receiver sends the IGMPv2 membership report to join the multicast group 225.1.1.1, and Source sends the multicast service packet with the multicast group 225.1.1.1.

#View the multicast member table 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
```

#Query the PIM-SM multicast route 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 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:

##You can see that the RPF neighbor from Device3 to multicast source is Device1, and the ingress interface of multicast service packet is vlan5.

#When the line between Device1 and Device3 fails, BFD will quickly detect and notify OSPF and PIM protocol, OSPF will switch the route to Device2 for communication, and notify PIM protocol of unicast route change, PIM protocol will quickly switch to the RPF neighbor of multicast source.

#View the PIM-SM neighbor and multicast roue table of device3.

```
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
```

#You can see that the RPF neighbor from Device3 to multicast source is switched to Device2, and the ingress interface of multicast service packet is vlan4.

Note

- Because the RPF route convergence of PIM and BFD linkage depends on the convergence speed of unicast routing, BFD also needs to link with the related unicast routing protocol OSPF.

7.8 MSDP

7.8.1 Overview

RP in the PIM-SM network only knows the multicast source information in the multicast domain, but in the actual application, the whole network is divided to multiple multicast domains. In the case, the RP in the domain cannot know the multicast source information out of the domain and the receiver cannot receive the multicast packets of other domains.

MSDP (Multicast Source Discovery Protocol) provides one multicast cross-domain solution. The MSDP mechanism transmits the multicast source information of the multicast domain to the RP of another multicast domain, and the RP in the other multicast domain can initiate adding to the multicast source of the multicast domain and set up the multicast distributing tree, so as to realize the cross-domain transmission of the multicast packets.

7.8.2 MSDP Function Configuration

Table 956 MSDP function configuration list

Configuration Task	
Configure the MSDP basic functions	Configure the MSDP peer
	Disable the MSDP peer
Configure the MSDP peer connection	Configure the default MSDP peer
	Configure the MSDP mesh group
Configure the SA packet	Configure the SA request packet
	Configure the SA packet filter policy

Note

- L3 Ethernet interface does not support the MSDP function.

7.8.2.1 Configure MSDP Peer

Set up the MSDP peer connection via the MSDP peer between the multicast

domains, forming one “MSDP interconnection map”. When the MSDP peer of one domain perceives the new multicast source, encapsulate the new multicast source information in the SA (Source-Active) packet and send to all remote peers setting up the MSDP peer connection. After MSDP peer receives the SA packet, the SA packet passing the RPF (Reverse Path Forwarding) is forwarded. With the relay between the MSDP peers, you can transmit the SA message sent by one RP to all the other RPs, realizing the sharing of the multicast source information between the multicast domains.

Use the TCP as the transmission protocol between the MSDP peers. Use the reliability of TCP to ensure that the MSDP protocol packets can be transmitted to the remote peer correctly.

Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast

Configure MSDP Peer

Set up the MSDP peer connection between the local device and the specified remote device. At the remote device, you also should specify the local device as the MSDP peer so that the peer connection can be set up successfully. After the peer connection is set up successfully, the peers interact the MSDP protocol packets via the connection.

Table 957 Configure the MSDP peer

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the MSDP peer	ip msdp [vrf *vrf-name*] peer *peer-ip-address* [connect-source *interface-name*] [remote-as *as-number-value*]	Mandatory By default, the MSDP peer is not configured.

Note

- When configuring the first MSDP peer, automatically enable the MSDP protocol.

Disable MSDP Peer

The administrator can disable the specified MSDP peer connection via the command according to the network demand. After disabling the MSDP peer connection, stop interacting the MSDP protocol packets between the MSDP peers.

Table 958 Disable the MSDP peer

Step	Command	Description
Enter global configuration mode	configure terminal	-
Disable the MSDP peer	ip msdp [vrf *vrf-name*] shutdown *peer-ip-address*	Mandatory By default, do not disable the MSDP peer.

7.8.2.2 Configure MSDP Peer Connection

After the device receives the SA packet, perform the RPF check. The packets passing the check are forwarded to the other peers that set up the peer connection. The

packets not passing the RPF check are dropped.

The default peer, mesh group can omit specifying the RPF check of the SA packet between the peers.

Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast
- Configure the MSDP peer

Configure Default MSDP Peer

When specifying the default MSDP peer, you can configure the RP range. When receiving the SA packet sent by the default peer and if the RP in the packet belongs to the permitted range, do not perform the RPF check. Otherwise, still perform the RPF check for the RP in the packet.

Table 959 Configure the default MSDP peer

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the default MSDP peer	ip msdp [vrf *vrf-name*] default-peer *peer-ip-address* [prefix-list *prefix-list-name*]	Mandatory By default, the MSDP default peer is not configured.

Configure MSDP Mesh Group

When receiving the SA packet from the peer in the group, the device directly passes the RPF check and does not forward the SA packet to the other peers in the

group, but just forwards to the peers out of the group. This can reduce the load of the device and avoid the repeated forwarding, so as to save the network bandwidth.

Table 960 Configure the MSDP mesh group

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the MSDP mesh group	ip msdp [vrf *vrf-name*] mesh-group *mesh-group-name peer-ip-address*	Mandatory By default, no peer is added to the mesh group.

7.8.2.3 Configure SA Packet

Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast
- Configure the MSDP peer

Configure SA Request Packet

After configuring the SA request packet on the device, the device immediately sends the SA request packet to MSDP peer when receiving the new multicast group adding packet, so as to reduce the adding delay of the multicast group.

Some RP does not hope to be known by the receivers of the un-recognized other multicast domain. You can configure the filter policy of the SA request packet on all peers of the multicast domain to which the RP belongs. Only answer the SA request packet of the peers permitted by the policy.

Table 961 Configure the SA request packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure sending the SA request packet	ip msdp [vrf *vrf-name*] sa-request *peer-ip-address*	Mandatory By default, when receiving the new multicast group adding packet, the device does not send the SA request packet to the MSDP peer, but waits for the SA packet of the next period.
Configure the filter policy of the received SA request packet	ip msdp [vrf *vrf-name*] filter-sa-request *peer-ip-address* [list *access-list-number* | *access-list-name*]	Mandatory By default, do not filter the SA request packet.

Note

- **ip msdp filter-sa-request** only supports the standard ACL.

Configure SA Packet Filter Policy

Usually, the MSDP peer accepts the SA packets from all peers that pass the RPF check and forward to all the peers out of the mesh group. The user can configure the filter policy of the SA packet on the peer as desired, controlling the SA packets from or sent to the specified peer. When receiving or forwarding the SA packet, the device filters the multicast source group and RP of the SA packet.

Table 962 Configure the filter policy of the SA packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the filter policy of the SA packet	ip msdp [vrf *vrf-name*] sa-filter { in | out } *peer-ip-address* [list { *access-list-name* | *access-list-number* }] [rp-list { *access-list-name* | *access-list-number* }]	Mandatory By default, do not filter the SA packet.

Note

- The **list** parameter of **ip msdp sa-filter** only supports the extended ACL.
- The **rp-list** parameter of **ip msdp sa-filter** only supports the standard ACL.

7.8.2.4 MSDP Monitoring and Maintaining

Table 963 MSDP Monitoring and Maintaining

Command	Description
clear ip msdp [vrf *vrf-name*] peer [*peer-ip-address*]	Clear the MSDP peer information
clear ip msdp [vrf *vrf-name*] sa-cache [*group-ip-address*]	Clear the SA cache information
clear ip msdp [vrf *vrf-name*] statistics [*peer-ip-address*]	Clear the statistics information of the MSDP peers
show ip msdp [vrf *vrf-name*] count [*as-number-value*]	Display the SA information received by MSDP from the AS domain
show ip msdp [vrf *vrf-name*] peer [*peer-ip-address* [*accepted-SAs* | *advertised-SAs*]]	Display the MSDP peer information
show ip msdp [vrf *vrf-name*] rpf [*peer-ip-address*]	Display the MSDP next-hop route information
show ip msdp [vrf *vrf-name*] sa-cache [*group-ip-address* [*source-ip-address*]] [*as-number-*	Display the MSDP SA cache information

Command	Description
value]	
show ip msdp [vrf *vrf-name*] summary	Display the summery information of the MSDP peer

7.8.3 MSDP Typical Configuration Example

7.8.3.1 Configure Inter-PIM-SM Domain Multicast

Network Requirements

- The whole network includes two AS: AS100 and AS200. Run the BGP protocol between Ass and use MBGP to interact the multicast route; in AS, run the OSPF protocol to interact the route.
- Multicast domain PIM-SM1 is located in AS100; multicast domain PIM-SM2 is located in AS200. Source is one multicast source of PIM-SM1. Receiver is one receiver of PIM-SM2.
- Loopback1 of Device2 is C-BSR of PIM-SM1 and Loopback0 of Device2 is C-RP of PIM-SM1. Loopback1 of Device3 is C-BSR of PIM-SM2 and Loopback0 of Device3 is C-RP of PIM-SM2.
- Between Device2 and Device3, set up the MSDP peer connection, so as to realize the cross-domain forwarding of the multicast service packet, so that Receiver can receive the multicast service packet sent by Source.

Network Topology

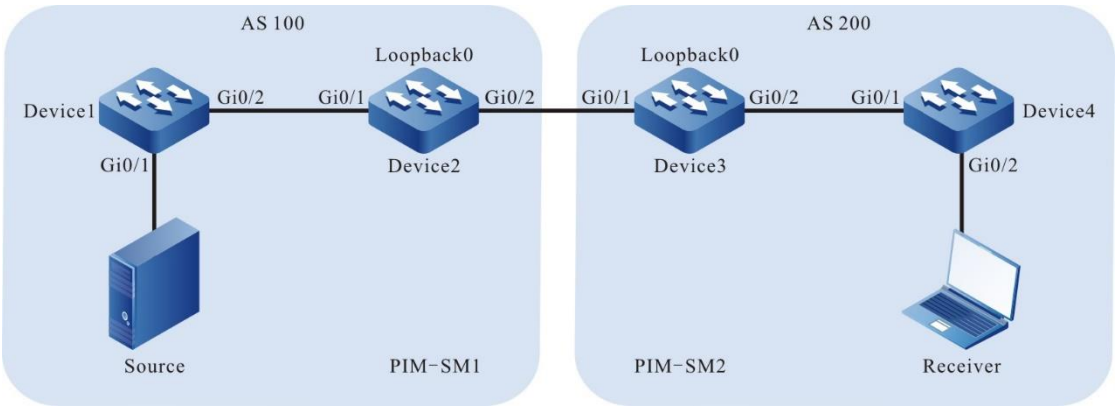


Figure 193 Networking of configuring the inter-PIM-SM domain multicast

Device	Interface	VLAN	IP Address
Device1	Gi0/1	2	10.1.1.1/24
	Gi0/2	3	10.1.2.1/24
Device2	Gi0/1	3	10.1.2.2/24
	Gi0/2	4	10.1.3.1/24
	Loopback0		11.11.11.11/32
	Loopback1		12.12.12.12/32
Device3	Gi0/1	4	10.1.3.2/24
	Gi0/2	5	10.1.4.1/24
	Loopback0		22.22.22.22/32
	Loopback1		12.12.12.12/32
Device4	Gi0/1	5	10.1.4.2/24
	Gi0/2	6	10.1.5.1/24
Source			10.1.1.2/24

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 OSPF so that all devices in the AS domain can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
```

```
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 12.12.12.12 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device3(config-ospf)#network 23.23.23.23 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(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   10.1.1.0/24 is directly connected, 00:05:44, vlan2
C   10.1.2.0/24 is directly connected, 22:24:35, vlan3
O   11.11.11.11/32 [110/2] via 10.1.2.2, 01:21:25, vlan3
O   12.12.12.12/32 [110/2] via 10.1.2.2, 01:19:25, vlan3
```

#View the route 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

C   10.1.4.0/24 is directly connected, 22:41:14, vlan5
C   10.1.5.0/24 is directly connected, 00:08:11, vlan6
O   22.22.22.22/32 [110/2] via 10.1.4.1, 01:23:33, vlan5
O   23.23.23.23/32 [110/2] via 10.1.4.1, 01:19:33, vlan5
```

You can see that Device1 and Device4 only learn the routes of the belonging AS domain.

Note

- The viewing method of Device2 and Device3 is the same as that of Device1, Device4, so the viewing process is omitted.

Step 4: Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure C-BSR and C-RP.

#Configure Device1.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the 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
```

#Configure Device2.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback1 as C-BSR and Loopback0 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ip pim sparse-mode
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback 1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exit
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
Device2(config)#ip pim bsr-candidate loopback1
Device2(config)#ip pim rp-candidate loopback0
```

#Configure Device3.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback1 as C-BSR and Loopback 0 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface loopback 1
Device3(config-if-loopback1)#ip pim sparse-mode
Device3(config-if-loopback1)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#ip pim bsr-candidate loopback 1
Device3(config)#ip pim rp-candidate loopback0
```

#Configure Device4.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the interfaces.

```
Device4(config)#ip multicast-routing
Device4(config)#interface vlan 5
Device4(config-if-vlan5)#ip pim sparse-mode
Device4(config-if-vlan5)#exit
Device4(config)#interface vlan 6
Device4(config-if-vlan6)#ip pim sparse-mode
Device4(config-if-vlan6)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device4 and the PIM-SM neighbor information.

```
Device4#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
10.1.4.2        register_vif0            1       v2/S   UP
10.1.4.2        vlan5                    0       v2/S   UP     1      1      10.1.4.2    FALSE  FALSE
10.1.5.1        vlan6                    2       v2/S   UP     0      1      10.1.5.1    FALSE  FALSE

Device4#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor        Interface                Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.1.4.1        vlan5                    23:03:12/00:01:20 v2    1 /
```

Note

- The viewing method of Device1, Device2, and Device3 is the same as that of Device4, so the viewing process is omitted.

#View the BSR and RP information of Device4.

```
Device4#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 23.23.23.23
  BSR Priority: 0
  Hash mask length: 10
  Up time: 01:57:44
  Expiry time: 00:01:28
  Role: Non-candidate BSR
  State: Accept Preferred

Device4#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: 22.22.22.22
      Info source: 23.23.23.23, via bootstrap, priority 192
      Up time: 01:57:45
      Expiry time: 00:01:47
```

#View the BSR and RP information of Device1.

```
Device1#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 12.12.12.12
  BSR Priority: 0
  Hash mask length: 10
  Up time: 02:00:24
  Expiry time: 00:01:44
  Role: Non-candidate BSR
  State: Accept Preferred

Device1#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: 11.11.11.11
      Info source: 12.12.12.12, via bootstrap, priority 192
      Up time: 02:00:30
      Expiry time: 00:01:58
```

You can see that there is only the BSR and RP information of the belonging multicast domain on Device4, Device1.

Note

- The viewing method of Device2 and Device3 is the same as that of Device1, Device4, so the viewing process is omitted.

Step 5: Configure MP-EBGP. Set up the direct-connected EBGP peer

between Device2 and Device3 and use the MBGP to interact the multicast route.

#Configure Device2.

Configure setting up the direct-connected EBGP peer with Device3, enable Multicast address stack and advertise the multicast route.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.1.3.2 remote-as 200
Device2(config-bgp)#address-family ipv4 multicast
Device2(config-bgp-af)#network 10.1.1.0 255.255.255.0
Device2(config-bgp-af)#network 11.11.11.11 255.255.255.255
Device2(config-bgp-af)#neighbor 10.1.3.2 activate
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#Configure Device3.

Configure setting up the direct-connected EBGP peer with Device2, enable Multicast address stack and advertise the multicast route.

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 10.1.3.1 remote-as 100
Device3(config-bgp)#address-family ipv4 multicast
Device3(config-bgp-af)#network 10.1.5.0 255.255.255.0
Device3(config-bgp-af)#network 22.22.22.22 255.255.255.255
Device3(config-bgp-af)#neighbor 10.1.3.1 activate
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

#View the BGP neighbor status of Device3.

```
Device3#show ip bgp summary
BGP router identifier 22.22.22.22, 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
10.1.3.1        4   100     114     111        2    0    0 01:35:00        0

Total number of neighbors 1
```

According to the number displayed in the State/PfxRcd list (the number of the

unicast route prefixes received from the neighbor), we can see that the BGP neighbor is set up between Device3 and Device2 successfully.

#View the BGP Multicast route table of Device3.

```
Device3#show bgp ipv4 multicast
BGP table version is 9, local router ID is 22.22.22.22
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]*> 10.1.1.0/24    10.1.3.1                 2             0 100 i
[B]*> 10.1.5.0/24    10.1.4.2                 2         32768 i
[B]*> 11.11.11.11/32 10.1.3.1                 0             0 100 i
[B]*> 22.22.22.22/32 0.0.0.0                  0         32768 i
```

You can see that Device3 learns the Source and RP routes of the multicast domain PIM-SM1 and the next hop is MSDP peer 10.1.3.1.

Note

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

Step 6: Configure MSDP.

#Configure Device2.

Configure setting up the direct-connected EBGP peer with Device3; enable the function of actively sending the SA request packet to the specified peer; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device2(config)#ip msdp peer 10.1.3.2 remote-as 200
Device2(config)#ip msdp sa-request 10.1.3.2
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device3.

Configure setting up the direct-connected EBGP peer with Device2; enable the function of actively sending the SA request packet to the specified peer; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device3(config)#ip msdp peer 10.1.3.1 remote-as 100
Device3(config)#ip msdp sa-request 10.1.3.1
Device3(config)#ip msdp rpf rfc3618
```

#View the MSDP peer connection status and details of Device3.

```
Device3#show ip msdp summary
MSDP Peer Status Summary
Total 1 Peer entry
Peer Address     AS     State     Reset   Uptime/Downtime
10.1.3.1         100    Up        0       02:21:18
Device3#show ip msdp peer
MSDP Peer Table:
Total 1 Peer entry
MSDP Peer 10.1.3.1, AS 100 (configured AS)
  Connection status:
    State: Established, Resets: 0, Connection source: none configured
    Uptime(Downtime): 02:50:00, Message sent/received: 136/161
    Connection and counters cleared 02:13:25 ago
    Local Address of connection: 10.1.3.2
    Remote Address of connection: 10.1.3.1
    Local Port: 639, Remote Port: 1179
  SA-Requests:
    Input filter: none
    Sending SA-Requests to peer: enabled
  SA:
    Input filter: none
  Message counters:
    RPF Failure count: 0
    SA Messages in/out: 47/0
    SA Requests in/out: 0/3
    SA Responses in/out: 3/0
  Data Packets in/out: 0/0
```

You can see that the MSDP peer connection is set up successfully between Device3 and Device2.

Note

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

Step 7: Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1; Source sends the multicast service packet with multicast group 225.1.1.1.

#View the multicast member table on Device4.

```
Device4#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                    00:05:11 00:02:38 10.1.5.2        stopped
```

#View the MSDP SA cache information of Device2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Originated, 00:11:45/00:05:39
```

You can see that Device2 generates and caches the SA packet. The multicast source address in the SA packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 11.11.11.11.

#View the MSDP SA cache information and RPF check table of Device3.

```
Device3#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 10.1.3.1, 00:08:39/00:05:21

Device3#show ip msdp rpf
Destination     Nexthop        Nexthop         Nexthop Metric  Pref
Address         Address        From            RefCnt
10.1.3.1        0.0.0.0        0.0.0.0         1       10      0
11.11.11.11     10.1.3.1       10.1.3.1        1       0       20
```

You can see that Device3 receives and caches the SA packet. The SA packet is from the peer 10.1.3.1. The multicast source address in the packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 11.11.11.11; the next hop of on the best path from Device3 to source end RP (11.11.11.11) is 10.1.3.1.

#View the PIM-SM multicast route 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 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(*, 225.1.1.1)
Up time: 00:13:57
RP: 22.22.22.22
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  vlan5 00:13:57/00:02:33
 Asserted interface list:

(10.1.1.2, 225.1.1.1)
Up time: 00:13:57
KAT time: 00:03:28
RPF nbr: 10.1.3.1
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 6906038

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:13:57
RP: 22.22.22.22
Flags:
 RPT JOIN DESIRED
 PRUNE DESIRED
 RPF SGRPT XG EQUAL
Upstream State: PRUNED

```
Local interface list:
Pruned interface list:
Outgoing interface list:
 vlan5
```

#Receiver can receive the multicast service packet with multicast group 225.1.1.1 sent by Source.

Note

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

7.8.3.2 Configure Anycast RP

Network Requirements

- The whole PIM multicast domain runs the PIM-SM protocol.
- Loopback0 interface of Device3 is C-BSR. Loopback1 interfaces of Device2 and Device4 are C-RP and the IP addresses are the same.
- Use the IP address of Loopback0 between Device2 and Device4 to set up the MSDP peer connection.
- In the domain, configure multiple RPs with the same address; non-RP device selects the nearest RP used to manage the multicast source and receiver. The RPs exchange the multicast source information via MSDP so that the multicast service of the whole multicast domain can be interacted. If one RP fails, its managed areas are shared by other RPs.

Network Topology

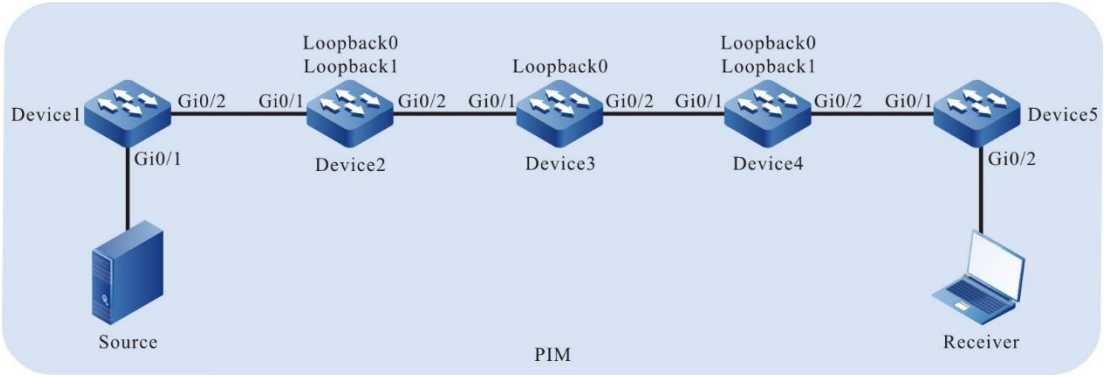


Figure 194 Networking of configuring Anycast RP

Device	Interface	VLAN	IP address
Device1	Gi0/1	2	10.1.1.1/24
	Gi0/2	3	10.1.2.1/24
Device2	Gi0/1	3	10.1.2.2/24
	Gi0/2	4	10.1.3.1/24
	Loopback0		11.11.11.11/32
	Loopback1		55.55.55.55/32
Device3	Gi0/1	4	10.1.3.2/24
	Gi0/2	5	10.1.4.1/24
	Loopback0		44.44.44.44/32
Device4	Gi0/1	5	10.1.4.2/24
	Gi0/2	6	10.1.5.1/24
	Loopback0		22.22.22.22/32
	Loopback1		55.55.55.55/32
Device5	Gi0/1	6	10.1.5.2/24
	Gi0/2	7	10.1.6.1/24
Source	-		10.1.1.2/24

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 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 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device4(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device5(config-ospf)#network 10.1.6.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

#View the route 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   10.1.1.0/24 [110/5] via 10.1.5.1, 04:04:37, vlan6
O   10.1.2.0/24 [110/4] via 10.1.5.1, 04:05:13, vlan6
O   10.1.3.0/24 [110/3] via 10.1.5.1, 04:17:36, vlan6
O   10.1.4.0/24 [110/2] via 10.1.5.1, 18:19:08, vlan6
C   10.1.5.0/24 is directly connected, 18:22:13, vlan6
C   10.1.6.0/24 is directly connected, 04:32:51, vlan7
O   11.11.11.11/32 [110/4] via 10.1.5.1, 04:17:36, vlan6
O   22.22.22.22/32 [110/2] via 10.1.5.1, 03:56:25, vlan6
O   44.44.44.44/32 [110/3] via 10.1.5.1, 04:13:23, vlan6
O   55.55.55.55/32 [110/2] via 10.1.5.1, 04:17:36, vlan6
```

Note

- The viewing method of Device1, Device2, Device3, and Device4 is the same as that of Device5, so the viewing process is omitted.

Step 4: Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure C-BSR and C-RP.

#Configure Device1.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the interface.

```
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
```

#Configure Device2.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM

on the interface, and configure Loopback1 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback0
Device2(config-if-loopback0)#ip pim sparse-mode
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exit
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
Device2(config)#ip pim rp-candidate loopback1
```

#Configure Device3.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback0 as C-BSR.

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ip pim sparse-mode
Device3(config-if-vlan4)#exit
Device3(config)#interface vlan 5
Device3(config-if-vlan5)#ip pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#ip pim bsr-candidate loopback0
```

#Configure Device4.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback1 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device4(config)#ip multicast-routing
Device4(config)#interface loopback0
Device4(config-if-loopback0)#ip pim sparse-mode
Device4(config-if-loopback0)#exit
```

```
Device4(config)#interface loopback1
Device4(config-if-loopback1)#ip pim sparse-mode
Device4(config-if-loopback1)#exit
Device4(config)#interface vlan 5
Device4(config-if-vlan5)#ip pim sparse-mode
Device4(config-if-vlan5)#exit
Device4(config)#interface vlan 6
Device4(config-if-vlan6)#ip pim sparse-mode
Device4(config-if-vlan6)#exit
Device4(config)#ip pim rp-candidate loopback1
```

#Configure Device5. Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

```
Device5(config)#ip multicast-routing
Device5(config)#interface vlan 6
Device5(config-if-vlan6)#ip pim sparse-mode
Device5(config-if-vlan6)#exit
Device5(config)#interface vlan 7
Device5(config-if-vlan7)#ip pim sparse-mode
Device5(config-if-vlan7)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device5 and the PIM-SM neighbor information.

```
Device5#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
10.1.5.2        register_vif0            1      v2/S   UP
10.1.5.2        vlan6                    0      v2/S   UP    1      1     10.1.5.2      FALSE  FALSE
10.1.6.1        vlan7                    2      v2/S   UP    0      1     10.1.6.1      FALSE  FALSE

Device5#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor        Interface                Uptime/Expires    Ver   DR
Address                                                          Priority/Mode
```

```
10.1.5.1        vlan6                18:37:22/00:01:45 v2    1 /
```

#View the BSR and RP information of Device5.

```
Device5#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 44.44.44.44
  BSR Priority: 0
  Hash mask length: 10
  Up time: 04:36:44
  Expiry time: 00:01:35
  Role: Non-candidate BSR
  State: Accept Preferred
Device5#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: 55.55.55.55
      Info source: 44.44.44.44, via bootstrap, priority 192
      Up time: 04:36:44
      Expiry time: 00:01:53
```

Note

- The viewing method of Device1, Device2, Device3, and Device4 is the same as that of Device5, so the viewing process is omitted.

Step 5: Configure MSDP.

#Configure Device2.

Configure setting up the non-direct-connected MSDP peer connection via Loopback0 with Loopback0 of Device4; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the

IP address of Loopback0; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device2(config)#ip msdp peer 22.22.22.22 connect-source loopback0
Device2(config)#ip msdp sa-request 22.22.22.22
Device2(config)#ip msdp originator-id loopback0
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device4.

Configure setting up the non-direct-connected MSDP peer connection via Loopback0 with Loopback0 of Device2; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the IP address of Loopback0; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device4(config)#ip msdp peer 11.11.11.11 connect-source loopback0
Device4(config)#ip msdp sa-request 11.11.11.11
Device4(config)#ip msdp originator-id loopback0
Device4(config)#ip msdp rpf rfc3618
```

#View the MSDP peer connection status and details of Device4.

```
Device4#show ip msdp summary
MSDP Peer Status Summary
Total 1 Peer entry
Peer Address     AS     State    Reset  Uptime/Downtime
11.11.11.11      ?      Up       0      05:49:35

Device4#show ip msdp peer
MSDP Peer 11.11.11.11, AS ?
  Connection status:
    State: Established, Resets: 0, Connection source: loopback0
    Uptime(Downtime): 05:49:39, Message sent/received: 352/528
    Connection and counters cleared 05:53:24 ago
    Local Address of connection: 22.22.22.22
    Remote Address of connection: 11.11.11.11
    Local Port: 639, Remote Port: 1053
  SA-Requests:
    Input filter: none
    Sending SA-Requests to peer: enabled
  SA:
    Input filter: none
  Message counters:
    RPF Failure count: 3
```

```
    SA Messages in/out: 348/0
    SA Requests in/out: 0/3
    SA Responses in/out: 2/0
  Data Packets in/out: 0/0
```

You can see that Device4 and Device2 set up the MSDP peer connection successfully.

Note

- The viewing method of Device2 is the same as that of Device4, so the viewing process is omitted.

Step 6: Check the result.

Source sends the multicast service packet with multicast group 225.1.1.1.

#View the MSDP SA cache information of Device2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 55.55.55.55, Originated, 00:03:34/00:05:43
```

You can see that Device2 generates and caches the SA packet. The multicast source address in the SA packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 55.55.55.55.

#View the MSDP SA cache information and RPF check table of Device4.

```
Device4#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 11.11.11.11, 00:07:02/00:05:58

Device4#show ip msdp rpf
Destination     Nexthop        Nexthop         Nexthop Metric  Pref
Address         Address        From            RefCnt
10.1.4.1        0.0.0.0        0.0.0.0         1       10      0
11.11.11.11     10.1.4.1       55.55.55.55     3       3       110
55.55.55.55     0.0.0.0        0.0.0.0         2       1       0
```

You can see that Device4 receives and caches the SA packet. The SA packet is from the peer 11.11.11.11. The multicast source address in the packet is 10.1.1.2; the

multicast group address is 225.1.1.1; the RP address is 11.11.11.11.

Note

- If **ip msdp originator-id** is configured on the source RP and when it sends the SA packet to MSDP peer, it replaces the RP address in the packet with the IP address of the specified interface.

#View the PIM-SM multicast route table of Device2.

```
Device2#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 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(10.1.1.2, 225.1.1.1)
Up time: 00:01:14
KAT time: 00:03:23
RPF nbr: 10.1.2.1
RPF idx: vlan3
SPT bit: FALSE
Flags:
Upstream State: NOT JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
  Packet count 0

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:01:14
RP: 55.55.55.55
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
```

```
Local interface list:
Pruned interface list:
Outgoing interface list:
```

#View the PIM-SM multicast route table of Device4.

```
Device4#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
```

You can see that there is (10.1.1.2, 225.1.1.1) entry on Device2 and no (10.1.1.2, 225.1.1.1) entry on Device4. It indicates that Source initiates the PIM-SM register to the nearest RP, that is, Device2.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1.

#View the multicast member table on Device5.

```
Device5#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        vlan7                    00:00:12 00:04:12 10.1.6.2        stopped
```

#View the PIM-SM multicast route table of Device2.

```
Device2#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 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(10.1.1.2, 225.1.1.1)
```

```
Up time: 00:19:01
KAT time: 00:03:14
RPF nbr: 10.1.2.1
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    vlan4 00:02:56/00:02:34
  Asserted interface list:
  Outgoing interface list:
    vlan4
  Packet count 1136269

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:19:01
RP: 55.55.55.55
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
```

#View the PIM-SM multicast route table of Device4.

```
Device4#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: 00:05:54
RP: 55.55.55.55
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
```

```
    vlan6  00:05:54/00:02:36
  Asserted interface list:

(10.1.1.2, 225.1.1.1)
Up time: 00:05:54
KAT time: 00:03:22
RPF nbr: 10.1.4.1
RPF idx: vlan5
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    vlan6  00:05:54/00:02:37
  Asserted interface list:
  Outgoing interface list:
    vlan6
  Packet count 2172581

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:05:54
RP: 55.55.55.55
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    vlan6
```

You can see that there is (*,225.1.1.1) entry on Device4 and no (*,225.1.1.1) entry on Device2. It indicates that Source initiates the PIM-SM adding to the nearest RP, that is, Device4.

#Receiver can receive the multicast service packet with multicast group 225.1.1.1 sent by Source.

7.9 MLD

7.9.1 Overview

MLD is short for Multicast Listener Discovery Protocol, used to set up and maintain the multicast group member relation between the IPv6 host and its direct neighboring multicast device. MLD router uses the IPv6 unicast link local address as the source address to send the MLD packet.

MLD router uses the local address of the IPv6 unicast link as the source address to send the MLD packet. All MLD packets are limited on the local link, and the hops are 1.

MLD has two versions: MLDv1n corresponds to IGMPv2, and MLDv2 corresponds to IGMPv3.

The packet types of the IGMP protocol adopting the IP protocol number 2 are different. The MLD protocol adopts the ICMPv6 (IP protocol number is 58) packet type, including MLD query packet (type value is 130), MLDv1 report packet (type value is 131), MLDv1 leave packet (type value is 132), and MLDv2 report packet (type value is 143). The MLD protocol and IGMP protocol have different packet formats, but have the same protocol actions.

7.9.2 MLD Function Configuration

7.9.2.1 Configure MLD Basic Functions

Configuration Condition

Before configuring the MLD basic functions, first complete the following task:

- Enable the interface IPv6
- Enable the interface MLD

Enable the MLD Protocol

Table 964 Enable the MLD protocol

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the IPv6 multicast forwarding	ipv6 multicast-routing [vrf *vrf-name*]	Mandatory By default, the IPv6 multicast forwarding is disabled.
Enter the interface configuration mode	interface *interface-name*	-
Enable the MLD protocol	ipv6 mld enable	Mandatory By default, do not enable MLD. After enabling MLD, all MLD configurations can take effect.

Configure the MLD Version

Table 965 Configure the MLD version

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the MLD version	ipv6 mld version *version-number*	Mandatory By default, the MLD version is 2.

Caution

- Because the packet structure and kind of different versions of MLD protocols are different, it is suggested to configure the same version of IGMP for all devices on the same subnet.

Configure Static Group Adding

After configuring one static group or source group in the interface, the device

regards that the interface has the receiver of the multicast group or source group.

Table 966 Configure static group adding

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the static group adding	ipv6 mld static-group *group-ipv6-address* [*source-ipv6-address*]	Mandatory By default, the interface is not added to any multicast group or source group in the static mode.

Configure Multicast Group Filter

The interface configured with the MLD multicast group filter filters the group member relation report in the segment according to the ACL rules and only the group member relation report permitted by ACL is processed and the un-permitted is directly dropped. For the existing but not permitted by ACL multicast group, immediately delete the multicast group information.

Table 967 Configure multicast group filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the IGMP multicast group filter	ipv6 mld access-group { *access-list-number* | *access-list-name* }	Mandatory By default, the multicast group filter is not configured.

Note

- The ipv6 mld access-group command only supports the standard ACL.

7.9.2.2 Adjust and Optimize the MLD Network

Configuration Condition

Before adjusting and optimizing the MLD network, first complete the following tasks:

- Enable the IPv6 protocol
- Enable the MLD protocol on the interface

Configure Query Interval of General Group

MLD querier periodically sends the general group query packets to maintain the group member relation. You can modify the interval of sending the MLD general group query packets according to the actuality of the network.

Table 968 Configure the query interval of the general group

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the query interval of the general group	ipv6 mld query-interval *interval-value*	Optional By default, the interval of sending the MLD general group query packets is 125s.

Note

- The genera query intervals of the devices on the same segment should try to keep consistent.
- The general group query interval should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

Configure Robustness Factor

The robustness factor is used to prevent the packet loss.

Table 969 Configure the robustness factor

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the robustness factor	ipv6 mld robustness-variable *variable-value*	Optional By default, the robustness factor of the MLD querier is 2.

Note

- After configuring the robustness factor, the following parameters also change with the robustness parameters:
- Group member timeout = Robustness factor * general group query time + maximum response time;
- Other querier timeout = Robustness factor * general group query time + maximum response time/2;
- The larger the robustness factor, the larger the MLD group member timeout and other querier timeout. Set the value according to the actuality of the network.

Configure Maximum Response Time

The general group query packet sent by the querier contains the maximum

response time field and the receiver sends the group member relation report within the maximum response interval. If the receiver does not send the group member relation report within the maximum response time, the device regards that the subnet does not have the receiver of the multicast group and deletes the multicast group information immediately.

Table 970 Configure the maximum response time

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the maximum response time	ipv6 mld query-max-response-time *seconds*	Optional By default, the maximum response time of the MLD general group query is 10s.

Configure Specified Group Query

After the MLD querier receives the leave packet of one multicast group, send the specified group query packet to query the multicast group on the segment. The sending times of the packet depends on “Specified group query times”. This is to know whether the subnet has the members of the multicast group. If not receiving the member relation report of the multicast group after waiting for “maximum response time”, delete the information of the multicast group.

Table 971 Configure the specified group query

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the query interval of the specified	ipv6 mld last-member-query-interval *interval-value*	Optional By default, the interval of

Step	Command	Description
group		sending the specified group query packets is 1s.
Configure the query times of the specified group	ipv6 mld last-member-query-count *count-value*	Optional By default, the times of sending the specified group query packets is 2.

Configure Fast Leave

The end segment in the network only connects to one host, which performs the switching action of the multicast group frequently. To reduce the leave delay, you can configure the fast leave of the multicast group on the device.

After configuring the fast leave, the device receives the leave packet of one multicast group and checks whether the multicast group belongs to the fast leave range. If yes, the device does not send the specified group query packet to the segment anymore and deletes the information of the multicast group immediately.

Table 972 Configure the fast leave

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the source group range of the fast leave	ipv6 mld immediate-leave { *access-list-number* | *access-list-name* }	Mandatory By default, do not permit the fast leave of the multicast group

7.9.2.3 Configure the MLD SSM Mapping

Configuration Condition

Before configuring the MLD SSM mapping, first complete the following tasks:

- Enable the interface IPv6
- Enable the interface MLD

Configure the MLD SSM Mapping

To provide the IPv6 PIM-SM SSM service for the receiver not supporting MLDv2 in the IPv6 PIM-SM SSM network, we can configure the MLD SSM Mapping function on the device.

The user can configure the MLD SSM Mapping rule according to the demand of the network receiver. The group member relation report permitted by the rule is converted to the MLD non-member (IS_EX, TO_EX) relation report, and the multicast source address is the source address specified by the MLD SSM mapping rule.

Table 973 Configure the MLD SSM mapping

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable MLD SSM Mapping	ipv6 mld ssm-map enable [vrf *vrf-name*]	Mandatory By default, MLD SSM Mapping is not enabled.
Configure the MLD SSM Mapping rule	ipv6 mld ssm-map static { *access-list-number* | *access-list-name* } *source-ipv6-address* [vrf *vrf-name*]	Mandatory By default, there is no MLD SSM Mapping rule.

Note

- The ipv6 mld ssm-map static command only supports the extended ACL.

7.9.2.4 MLD Monitoring and Maintaining

Table 974 MLD monitoring and maintaining

Command	Description
clear ipv6 mld group [*group-ipv6-address*] [*interface-name*] [vrf *vrf-name*]	Clear the MLD multicast group information
clear ipv6 mld statistic interface	Clear the MLD packet statistics information on

Command	Description
interface-name	the interface
show ipv6 mld groups [[static] | [*interface-name*] [*group-ipv6-address*] [detail]] [vrf *vrf-name*]	Display the MLD multicast group information
show ipv6 mld interface [*interface-name*] [vrf *vrf-name*]	Display the interface MLD information
show ipv6 mld statistic interface *interface-name* [vrf *vrf-name*]	Display the statistics information of the MLD packets

7.9.3 MLD Typical Configuration Example

7.9.3.1 Configure MLD Basic Functions

Network Requirements

- The whole network runs the IPv6 PIM-SM protocol.
- Device1, Device2, and Receiver are in the same LAN and Device1 is the querier.
- Receiver is one receiver of Device1 and Device2 stub network.
- Run MLDv2 between Device1, Device2 and stub network.

Network Topology

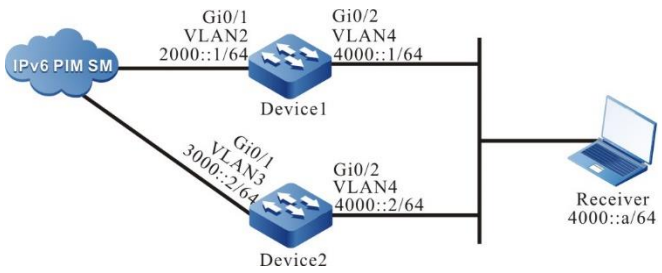


Figure 195 Networking of configuring MLD basic functions

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface (omitted).

Step 3: Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the interface. Enable MLD on the interface of Device1 and Device2 connecting the Receiver.

#Configure Device1.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol IPv6 PIM-SM on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device1#configure terminal
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#ipv6 mld enable
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol IPv6 PIM-SM on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device2#configure terminal
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 pim sparse-mode
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#ipv6 mld enable
Device2(config-if-vlan4)#exit
```

Step 4: Check the result.

#View the MLD version information and querier election result of Device1

interface vlan4.

```
Device1#show ipv6 mld interface vlan4
Interface vlan4 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

#View the MLD version information and querier election result of Device2 interface gigabitethernet0/0/1.

```
Device2#show ipv6 mld interface vlan4
Interface vlan4 (Index 50331674)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406
 Non-Querier: fe80::201:7aff:febc:662b Expires: 00:04:07
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

Receiver sends the MLDv2 member report packet to add to multicast group FF1E::1.

#View the multicast member table of Device1.

```
Device1#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface       Uptime    Expires  V1-Expires Last Reporter
ff1e::1      vlan4  00:00:02   00:04:17 not used   fe80::b
```

#View the multicast member table of Device2.

```
Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface       Uptime    Expires  V1-Expires Last Reporter
ff1e::1      vlan4  00:00:02   00:04:17 not used   fe80::b
```

Note

- On the interface, run the MLDv2 version, be compatible with the MLDv1 member relation report and MLDv1 member leave packet by default. You can configure the running MLD version of the interface via the command ipv6 mld version.
- When multiple devices run MLD in one LAN, elect the MLD querier and the one with the smallest address is elected as the MLD querier of the LAN.

7.9.3.2 Configure MLD Static Adding

Network Requirements

- The whole network runs the IPv6 PIM-SM protocol.
- Receiver is one receiver of the Device stub network.
- Run MLDv2 between Device and the stub network.
- Device interface vlan3 adds to multicast group FF1E::1 statically.

Network Topology

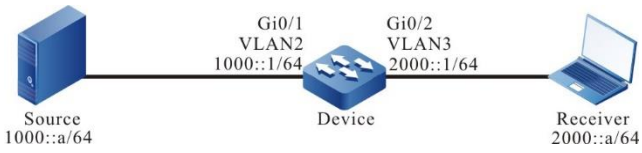


Figure 196 Networking of configuring MLD static adding

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface (omitted).

Step 3: Globally enable the IPv6 multicast forwarding, enable the multicast protocol IPv6 PIM-SM on the interface. Enable MLD on the interface of connecting the Receiver.

#Configure Device.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol IPv6 PIM-SM on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 pim sparse-mode
Device(config-if-vlan3)#ipv6 mld enable
Device(config-if-vlan3)#exit
```

#View the MLD information of Device interface vlan3.

```
Device#show ipv6 mld interface vlan3
Interface vlan3 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

Step 4: Device interface vlan3 adds to multicast group

FF1E::1 statically.

#Configure Device.

Device interface vlan3 adds to multicast group FF1E::1 statically.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 mld static-group ff1e::1
Device(config-if-vlan3)#exit
```

Step 5: Check the result.

#Source sends the multicast packet with multicast group FF1E::1.

#View the multicast member table of Device.

```
Device#show ipv6 mld groups
MLD Static Group Membership
Total 1 Static Groups
Group          Source         Interface
ff1e::1        ::             vlan3
```

#View the multicast route table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 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


(*, ff1e::1)
Up time: 00:01:06
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
Local interface list:
Vlan3
Joined interface list:
Asserted interface list:
```

(1000::a, ff1e::1)
Up time: 00:00:04
KAT time: 00:03:26
RPF nbr: ::
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

(1000::a, ff1e::1, rpt)
Up time: 00:00:04
RP: ::
Flags:
RPT JOIN DESIRED
RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:

#Receiver can receive the multicast packet with multicast group FF1E::1 sent by Source.

7.9.3.3 Configure MLD SSM Mapping

Network Requirements

- The whole network runs the IPv6 PIM-SM SSM protocol.
- Receiver1, Receiver2, and Device2 are all in one LAN.
- Run MLDv2 between Device2 and the stub network.
- Use the MLD SSM mapping on Device2 so that Receiver2 can only receive

the multicast service packets sent by Source1.

Network Topology

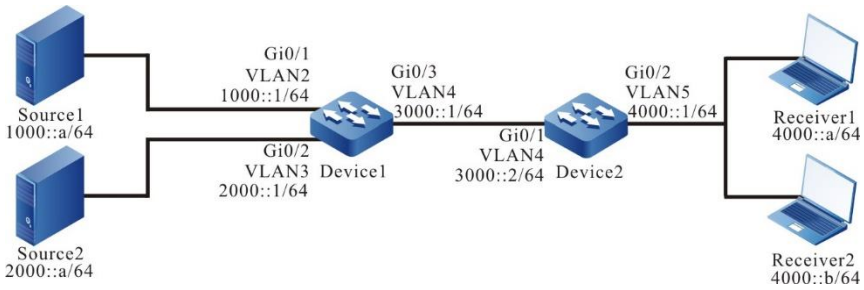


Figure 197 Networking of configuring the MLD SSM mapping

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface (omitted).

Step 3: Enable the IPv6 unicast routing OSPFv3 so that all network devices in the network can communicate with each other.

#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 vlan4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
```

#View the route 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 ::, 05:20:37, lo0
O   1000::/64 [110/2]
     via fe80::201:2ff:fe03:406, 00:35:30, vlan4
O   2000::/64 [110/2]
     via fe80::201:2ff:fe03:406, 00:37:15, vlan4
C   3000::/64 [0/0]
     via ::, 00:38:24, vlan4
L   3000::2/128 [0/0]
     via ::, 00:38:22, lo0
C   4000::/64 [0/0]
     via ::, 00:31:55, vlan5
L   4000::2/128 [0/0]
     via ::, 00:31:53, lo0
```

Note

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.

Step 4: Enable the IPv6 multicast forwarding globally, configure IPv6 PIM-SM SSM globally and the multicast group range of the SSM service is FF3X::/32. On the interfaces, enable the multicast protocol IPv6 PIM-SM. The interface vlan5 of Device2 runs

MLDv2.

#Configure Device1.

Enable the IPv6 multicast forwarding globally, configure the IPv6 PIM-SM SSM globally and enable the multicast protocol IPv6 PIM-SM on the interface.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#ipv6 pim ssm default
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Enable the IPv6 multicast forwarding globally, configure the IPv6 PIM-SM SSM globally, enable the multicast protocol IPv6 PIM-SM on the related interfaces, and run MLDv2 on the interface vlan5.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#ipv6 pim ssm default
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
Device2(config-if-vlan5)#ipv6 mld enable
Device2(config-if-vlan5)#exit
```

#View the MLD information of the interface vlan5 on Device2.

```
Device2#show ipv6 mld interface vlan5
Interface vlan5 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
```

```
Querier timeout is 255 seconds
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
Robustness variable is 2
```

Step 5: Enable the MLD SSM mapping on Device2 and configure the MLD SSM mapping rule so that Receiver1 and Receiver2 can only receive the multicast packets sent by Source1.

#Configure Device2.

Enable the MLD SSM mapping, configure the multicast group range of the MLD SSM as FF3E::/64, and the multicast source address is 1000::a.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#permit ipv6 any ff3e::/64
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ipv6 mld ssm-map enable
Device2(config)#ipv6 mld ssm-map static 7001 1000::a
```

Step 6: Check the result.

Receiver1 sends the MLDv2 member report packet of the specified source group to add to the multicast group FF3E::1 and the specified multicast source is 2000::a; Receiver2 sends the MLDv1 member report packet to add to the multicast group FF3E::2.

#Source1 and Source2 both send the multicast service packets with multicast groups FF3E::1 and FF3E::2.

#View the multicast member table of Device2.

```
Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group              Interface        Uptime    Expires  V1-Expires Last Reporter
ff3e::1            vlan5            00:00:33  not used not used   fe80::a
ff3e::2            vlan5            00:00:33  not used not used   fe80::b
```

```
Device2#show ipv6 mld groups detail
MLD Connected Group Membership
Total 2 Connected Groups
Group              Interface        Uptime    Expires  V1-Expires Last Reporter
ff3e::1            vlan5            00:00:36   not used not used   fe80::a
 Group mode : Include
 TIB-A Count: 1
 TIB-B Count: 0

 TIB-A
 Source list: (R - Remote, M - SSM Mapping)
 Source                          Uptime    Expires  Flags
 2000::a                         00:00:36   00:03:49 R
ff3e::2            vlan5            00:00:36   not used not used   fe80::b
 Group mode : Include
 TIB-A Count: 1
 TIB-B Count: 0

 TIB-A
 Source list: (R - Remote, M - SSM Mapping)
 Source                          Uptime    Expires  Flags
 1000::a                         00:00:36   00:03:45 RM
```

#View the multicast route table of Device2.

```
Device2#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(2000::a, ff3e::1)
Up time: 00:01:36
KAT time: 00:01:54
RPF nbr: fe80::201:2ff:fe03:406
RPF idx: vlan4
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
```

```
    vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan5
  Packet count 0

(1000::a, ff3e::2)
Up time: 00:01:36
KAT time: 00:01:54
RPF nbr: fe80::201:2ff:fe03:406
RPF idx: vlan4
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan5
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan5
  Packet count 0
```

#Receiver1 can only receive the multicast service packets sent by Source2; Receiver2 can only receive the multicast service packets sent by Source1.

Note

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.
- MLD SSM mapping needs to be used with IPv6 PIM-SM SSM; the multicast group range in the MLD SSM mapping rule should belong to the IPv6 PIM-SM SSM multicast group range. IGMP SSM mapping mainly runs MLDv1 and cannot be upgraded to the receiver host of MLDv2 to provide the supporting for the SSM model.
- The MLD SSM mapping is invalid for the MLDv2 member report packet.

7.9.3.4 Configure MLD Multicast Group Filter

Network Requirements

- The whole network runs the IPv6 PIM-SM protocol.
- Receiver is one receiver of the Device stub network.
- Run MLDv2 between Device and the stub network.
- Device interface gigabitethernet0/0/1 filters the multicast group; the range of the multicast groups Receiver is permitted to add is ff10::/16.

Network Topology

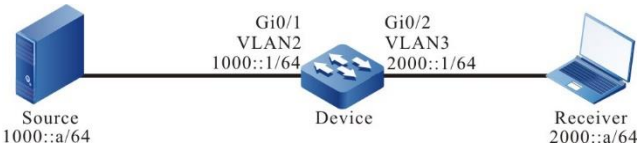


Figure 198 Networking of configuring IGMP multicast group filter

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface (omitted).

Step 3: Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the interface.

#Configure Device.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol IPv6 PIM-SM on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
```

```
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 pim sparse-mode
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 pim sparse-mode
Device(config-if-vlan3)#ipv6 mld enable
Device(config-if-vlan3)#exit
```

#View the MLD information of Device interface vlan3.

```
Device#show ipv6 mld interface vlan3
Interface vlan3 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

Step 4: Configure the multicast group filter on Device interface vlan3.

#Configure Device.

Configure the multicast group filter on Device interface vlan3; the range of the multicast groups Receiver is permitted to add is ff10::/16.

```
Device(config)#ipv6 access-list extended 7001
Device(config-std-nacl)#permit ipv6 any ff10::/16
Device(config-std-nacl)#commit
Device(config-std-nacl)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 mld access-group 7001
Device(config-if-vlan3)#exit
```

Step 5: Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group FF10::1 and FF11::1.

#Source sends the multicast packets with multicast group FF10::1 and FF11::1.

#View the multicast member table of Device.

```
Device#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group         Interface       Uptime    Expires  V1-Expires Last Reporter
ff10::1       vlan3  01:06:32   00:04:15 00:04:15   fe80::b
```

#View the multicast route table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 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

(*, ff10::1)
Up time: 00:01:00
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
  Local interface list:
    vlan3
  Joined interface list:
  Asserted interface list:

(1000::a, ff10::1)
Up time: 00:00:06
KAT time: 00:03:24
RPF nbr: ::
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
          vlan3
```

```
  Joined interface list:
    register_vif0
  Asserted interface list:
  Outgoing interface list:
register_vif0
vlan3
  Packet count 1

(1000::a, ff10::1, rpt)
Up time: 00:00:06
RP: ::
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:

(1000::a, ff11::1)
Up time: 00:00:06
KAT time: 00:03:24
RPF nbr: ::
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

(1000::a, ff11::1, rpt)
Up time: 00:00:06
RP: ::
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 service packets with multicast group FF10::1 sent by Source.

Note

- To filter based on multicast source group, use the command ipv6 mld access-group to realize, and configure the corresponding source address in the associated ACL. For example, permit ipv6 1000::/16 ff10::/16 indicates permitting the source group in the group range FF10::/16 and the specified source range 1000::/16 to add. When using the function, it is required that the interface runs MLDv2.

7.10 MLD snooping

7.10.1 Overview

MLD Snooping is short for Multicast Listener Discovery Snooping. It is an IPv6 multicast constraint mechanism running on L2 devices, used to manage and control IPv6 multicast groups.

MLD Snooping mainly realizes the following functions:

- Listen for MLD packets to establish multicast information. MLD Snooping obtains information about the downstream multicast receiver by listening for MLD packets and forwards multicast service packets on designated member ports.
- Listen for MLD packets. In this way, the upstream multicast router can correctly maintain the MLD member relation table.

7.10.2 MLD snooping Function Configuration

Table 975 MLD snooping function configuration list

Configuration Tasks	
Configure MLD snooping basic functions	Enable the MLD snooping function
	Configure the MLD snooping version

Configuration Tasks	
	Enable the MLD snooping MAC forwarding function
Configure MLD snooping querier	Enable the MLD snooping querier
	Configure the source IPv6 address of the MLD query packet
	Configure the query interval of the common group
	Configure the maximum response time
	Configure the query interval of the specified group
	Configure fast leave
Configure MLD snooping router port	Configure MLD snooping router port
	Configure the age time of the MLD snooping dynamic router port
Configure MLD snooping TCN event	Enable the fast convergence
	Configure the query interval of the TCN event
	Configure the query times of the TCN event

7.10.2.1 Configure MLD snooping Basic Functions

In the configuration tasks of MLD snooping, first enable the MLD snooping function so that the configurations of the other functions can take effect.

Configuration Condition

Before configuring the basic functions of MLD snooping, first complete the following tasks:

- Configure VLAN

Enable MLD snooping Function

After the MLD snooping function is enabled, the MLD snooping function can run on the device.

Table 976 Enable the MLD snooping function

Step	Command	Description

Enter global configuration mode	configure terminal	-
Enable the global MLD snooping function	ipv6 mld snooping	Mandatory By default, do not enable the global MLD snooping function.
Enable the MLD snooping function of the specified VLAN	ipv6 mld snooping vlan *vlan-id*	Mandatory By default, do not enable the MLD snooping function in the VLAN.

Note

- After the global MLD snooping function is enabled, the MLD snooping function of the specified VLAN can be enabled.

Configure MLD snooping Version

The configured MLD snooping version and MLD protocol packet processing rules are as follows:

When the configured MLD snooping version is V2, the device can process the MLD protocol packets of V1 and V2.

When the configured MLD snooping version is V1, the device can process the MLD protocol packets of V1, but does not process the V2 protocol packets, which flood in the VLAN.

Table 977 Configure MLD snooping version

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the MLD snooping version	ipv6 mld snooping vlan *vlan-id* version *version-number*	Optional By default, the version of MLD snooping is 2.

Enable MLD snooping MAC Forwarding

Usually, MLD snooping forwards the multicast packets in the VLAN according to multicast source IP address and multicast destination IP address. After configuring MLD snooping MAC forwarding, MLD snooping forwards the multicast packets in the VLAN according to the multicast destination MAC address.

Table 978 Enable MLD snooping MAC forwarding

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the L2 multicast MAC forwarding function in the specified VLAN	ipv6 mld snooping vlan *vlan-id* l2-forwarding	Mandatory By default, enable MLD snooping L2 multicast IP forwarding function of VLAN.

7.10.2.2 Configure MLD snooping Querier

If there is no L3 multicast device in the network, it cannot realize the related functions of the MLD querier. To solve the problem, you can configure the MLD snooping querier on the L2 multicast device to realize the MLD querier function so that L2 multicast device can set up and maintain the multicast forwarding entry, so as to forward multicast service packets normally.

Configuration Condition

Before configuring the basic functions of MLD snooping, first complete the following tasks:

- Enable global and VLAN MLD snooping function.

Enable MLD snooping Querier

You should first enable the MLD snooping querier function so that the configuration of the other features of the querier can take effect.

Table 979 Enable the MLD snooping querier

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the MLD snooping querier	ipv6 mld snooping vlan *vlan-id* querier	Mandatory By default, do not enable the MLD snooping querier of the specified VLAN.

Configure IPv6 Address of the Querier

The querier configured with IPv6 address takes part in the election of the MLD querier in VLAN and the querier fills the IPv6 address in the source IPv6 address field of the sent MLD group query packet.

Table 980 Configure the IPv6 address of the querier

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the IPv6 address of the querier	ipv6 mld snooping vlan *vlan-id* querier address *ipv6-address*	Mandatory By default do not configure the querier IPv6 address of the specified VLAN.

Note

- When the querier IPv6 address is not configured, the default source IPv6 address of the querier is 0::0, but the querier does not send the MLD group query packet with source IPv6 address 0.0.0.0.

Configure Query Interval of General Group

MLD querier periodically sends the query packets of the general group to maintain the group member relation. You can modify the interval of sending the MLD 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 MLD protocol packets in the network, avoiding the network congestion.

Table 981 Configure the query interval of the general group

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the query interval of the general group	ipv6 mld snooping vlan *vlan-id* querier query-interval *interval-value*	Optional By default, the query interval of the general group is 125s.

Note

- In one VLAN, the configured query interval of the general group should be larger than the maximum response time. Otherwise, the configuration will fail.

Configure Max. Response Time

The general group query packet sent by MLD 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 982 Configure the maximum response time

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure the maximum response time	ipv6 mld 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 will fail.

Configure Query Interval of Specified Group

When the MLD 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 983 Configure the query interval of the specified group

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the query interval of the specified group	ipv6 mld snooping vlan *vlan-id* last-member-query-interval *interval-value*	Optional By default, the query interval of the specified group is 1000ms.

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 984 Configure fast leave

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure fast leave	ipv6 mld snooping vlan *vlan-id* immediate-leave	Mandatory By default, do not enable the fast leave function of the specified VLAN.

Note

- There are multiple receivers of the same multicast group in the device port at the same time. When the port receives the MLD 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.

7.10.2.3 Configure MLD snooping Router Port

MLD snooping router port is the port receiving MLD group query packets or multicast routing protocol packets. When the device receives the MLD member report or leave packet, forward the packet via MLD snooping router port. In this way, the upper-connected router can maintain the MLD member relation table correctly.

MLD snooping router port can be dynamically learned or configured manually. MLD snooping dynamic router port refreshes the age time by regularly receiving the MLD group query packets or multicast routing protocol packets. MLD snooping static router port will not be aged.

Configuration Condition

Before configuring the MLD snooping router port functions, first complete the following tasks:

- Enable global and VLAN MLD snooping function
- Add port member in VLAN

Configure MLD snooping Static Router Port

After configuring MLD snooping static router port, the device can forward the MLD protocol packet via the port even the port does not receive the MLD 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 985 Configure MLD snooping static router port

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure MLD snooping static router port	ipv6 mld snooping vlan *vlan-id* mrouter { interface *interface-name* | link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the MLD snooping static router port.

Configure Age Time of MLD snooping Dynamic Router Port

If the configured age time of the MLD 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 986 Configure age time of MLD snooping dynamic router port

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure age time of MLD snooping dynamic router port	ipv6 mld snooping vlan *vlan-id* timer router-port expiry *expiry-value*	Optional By default, the age time of MLD snooping dynamic router port is 255s.

7.10.2.4 Configure MLD snooping TCN Event

Configuration Condition

Before configuring the MLD snooping TCN event function, first complete the following task:

- Enable global and VLAN MLD snooping function

Enable Fast Convergence

When the network topology changes, generate the TCN event and the spanning tree root port actively sends the global IMGP leave packets to request the MLD querier to send the general group query packet, making the fast convergence.

After enabling MLD snooping TCN event fast convergence, non-spanning tree root port also actively sends the global MLD leave packet, making the fast convergence.

Table 987 Enable fast convergence

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable fast convergence	ipv6 mld snooping tcn query solicit	Mandatory By default, do not enable fast convergence in the TCN event.

Configure Query Interval of TCN Event

When the TCN event happens, MLD snooping querier sends the general group query according to the TCN event query interval.

Table 988 Configure query interval of TCN event

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure query interval of TCN event	ipv6 mld snooping vlan *vlan-id* querier tcn query interval *interval-value*	Optional By default, the query interval of the TCM event is 31s.

Configure Query Times of TCN Event

When the TCN event happens, MLD 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 989 Configure query times of TCN event

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the query times of the TCN event	ipv6 mld snooping vlan *vlan-id* querier tcn query count *count-number*	Optional By default, the query times of the TCN event is 2.

7.10.2.5 Configure IPv6 PIM-SM Basic Functions

Network Requirements

- The whole network runs the IPv6 PIM-SM protocol.
- Receiver1 and Receiver2 are the two receivers of Device3 stub network.
- Device1 and Device2 are C-BSR and C-RP.
- Run MLDv2 between Device3 and the stub network.

Network Topology

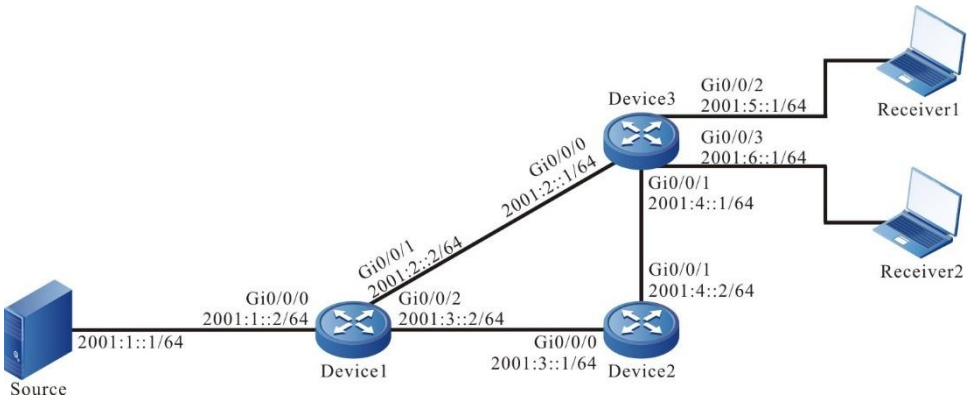


Figure 199 Networking of configuring IPv6 PIM-SM basic functions

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (omitted)

Step 2: Enable the unicast route protocol OSPFv3 so that all devices in the network can communicate with each other.

#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 gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/2)#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 gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
```

```
Device2(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/1)#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 gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
Device3(config-if-gigabitethernet0/0/3)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/3)#exit
```

#View the route 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 ::, 2w6d:04:39:46, lo0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
C   2001:2::/64 [0/0]
    via ::, 00:01:05, gigabitethernet0/0/0
L   2001:2::1/128 [0/0]
    via ::, 00:01:04, lo0
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
                [110/2]
    via fe80::201:7aff:fec0:525a, 00:00:04, gigabitethernet0/0/1
C   2001:4::/64 [0/0]
    via ::, 00:00:49, gigabitethernet0/0/1
L   2001:4::1/128 [0/0]
    via ::, 00:00:48, lo0
C   2001:5::/64 [0/0]
    via ::, 00:00:43, gigabitethernet0/0/2
L   2001:5::1/128 [0/0]
```

```
    via ::, 00:00:42, lo0
C   2001:6::/64 [0/0]
    via ::, 00:00:43, gigabitethernet0/0/3
L   2001:6::1/128 [0/0]
    via ::, 00:00:42, lo0
```

Note

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.

Step 3: Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
```

```
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
Device3(config-if-gigabitethernet0/0/3)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/3)#exit
```

#View the information of the interface enabled with the IPv6 PIM-SM protocol on Device3 and the IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 5 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF  Nbr   DR   BSR   CISCO   Neighbor
               Index  Mode  Flag  Count  Pri  Border Neighbor Filter
register_vif0   2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

gigabitethernet0/0/0        1     v2/S  UP   1    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d   Global Address: 2001:2::1      DR: fe80::201:7aff:fe62:bb7e

gigabitethernet0/0/1        3     v2/S  UP   1    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e   Global Address: 2001:4::1      DR: fe80::201:7aff:fec0:525a

gigabitethernet0/0/2        4     v2/S  UP   0    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f   Global Address: 2001:5::1      DR: fe80::201:7aff:fe5e:6d2f

gigabitethernet0/0/3        5     v2/S  UP   0    1    FALSE  FALSE
```

```
Address : fe80::201:7aff:fe5e:6d30    Global Address: 2001:6::1      DR: fe80::201:7aff:fe5e:6d30

Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor              Interface      Uptime/Expires     Ver   DR
Address                                                 Priority/Mode
fe80::201:7aff:fe62:bb7e gigabitethernet0/0/0      00:04:01/00:01:29   v2    1 / DR
fe80::201:7aff:fec0:525a gigabitethernet0/0/1      00:04:03/00:01:39   v2    1 / DR
```

Note

- The viewing methods of Device1 and Device2 are the same as that of Device3, so the viewing process is omitted.

Step 4: Enable MLD on gigabitethernet0/0/2 and gigabitethernet0/0/3 of Device3.

#Configure Device3.

Enable MLD on gigabitethernet0/0/2 and gigabitethernet0/0/3 of Device3.

```
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 mld enable
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
Device3(config-if-gigabitethernet0/0/3)#ipv6 mld enable
Device3(config-if-gigabitethernet0/0/3)#exit
```

#Query the MLD information of Device3 interface gigabitethernet0/0/2 and gigabitethernet0/0/3.

```
Device3#show ipv6 mld interface
Interface gigabitethernet0/0/2 (Index 11)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d2f (Self)
 Default version: 2
 Querier parameter:
   Query interval is 125 seconds
```

```
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
Interface gigabitethernet0/0/3 (Index 12)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d30 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

Note

- You can configure the MLD version running on the interface via the command ipv6 mld version.

Step 5: Configure interface gigabitethernet0/0/1 of Device1 as C-BSR and C-RP, and configure interface gigabitethernet0/0/0 of Device2 as C-BSR and C-RP.

#Configure Device1.

Configure interface gigabitethernet0/0/1 of Device1 as C-BSR and C-RP; the priority of C-BSR is 200; the multicast group range of the C-RP service is FF10::/16.

```
Device1(config)#ipv6 pim bsr-candidate gigabitethernet0/0/1 10 200
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 any ff10::/16
Device1(config-v6-list)#exit
Device1(config)#ipv6 pim rp-candidate gigabitethernet0/0/1 group-list 7001
```

#Configure Device2.

Configure interface gigabitethernet0/0/0 of Device2 as C-BSR and C-RP; the priority of C-BSR is 0; the multicast group range of the C-RP service of Device2 is FF00::/8.

```
Device2(config)#ipv6 pim bsr-candidate gigabitethernet0/0/0
Device2(config)#ipv6 pim rp-candidate gigabitethernet0/0/0
```

#View the BSR and RP information of Device3.

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:2::2
  BSR Priority: 200
  Hash mask length: 10
  Up time: 00:03:04
  Expiry time: 00:02:06
  Role: Non-candidate BSR
  State: Accept Preferred
Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): ff00::/8
  RP count: 1
    RP: 2001:3::1
      Info source: 2001:2::2, via bootstrap, priority 192
      Up time: 00:21:30
      Expiry time: 00:02:24

  Group(s): ff10::/16
  RP count: 1
    RP: 2001:2::2
      Info source: 2001:2::2, via bootstrap, priority 192
      Up time: 00:04:31
      Expiry time: 00:02:24
```

Caution

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- When configuring multiple C-BSRs in one multicast domain, first elect BSR according to the priority and the C-BSR with the largest priority is elected as BSR. When the priorities of C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR.
- When configuring multiple C-RPs in one multicast domain and the service multicast group ranges are the same, calculate the RP of the multicast group G according to the hash algorithm.
- In the multicast domain, you can configure RP via the command **ipv6 pim rp-address**, but it is required that the static RP addresses configured on all devices in the multicast domain keep consistent.

Step 7: Check the result.

#PC1 and PC2 send the MLDv2 member report packet to add to multicast group FF10::1 and FF50::1respectively.

#Source sends the multicast packets with multicast group FF10::1, FF50::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group    Interface        Uptime    Expires   V1-Expires   Last Reporter
ff10::1  gigabitethernet0/0/2          00:00:09  00:04:13  not used     fe80::210:94ff:fe00:1
ff50::1  gigabitethernet0/0/3          00:00:09  00:04:14  not used     fe80::210:94ff:fe00:2
```

#View the RP of multicast group FF10::1, FF50::1on Device3.

```
Device3#show ipv6 pim rp-hash ff10::1
 PIM6 VRF Name: Default
 RP: 2001:2::2
  Info source: 2001:2::2, via bootstrap
```

```
Device3#show ipv6 pim rp-hash ff50::1
  PIM6 VRF Name: Default
  RP: 2001:3::1
    Info source: 2001:2::2, via bootstrap
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 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
(*, ff10::1)
Up time: 00:00:06
RP: 2001:2::2
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet0/0/2
  Joined interface list:
  Asserted interface list:


(2001:1::1, ff10::1)
Up time: 00:00:05
KAT time: 00:03:25
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet0/0/2
  Packet count 0
```

(2001:1::1, ff10::1, rpt)
Up time: 00:00:05
RP: 2001:2::2
Flags:
 RPT JOIN DESIRED
 RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
 Local interface list:
 Pruned interface list:
 Outgoing interface list:

(*, ff50::1)
Up time: 00:00:06
RP: 2001:3::1
RPF nbr: fe80::201:7aff:fec0:525a
RPF idx: gigabitethernet0/0/1
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet0/0/3
 Joined interface list:
 Asserted interface list:

(2001:1::1, ff50::1)
Up time: 00:00:05
KAT time: 00:03:27
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet0/0/3
 Packet count 1

(2001:1::1, ff50::1, rpt)
Up time: 00:00:05
RP: 2001:3::1
Flags:
 RPT JOIN DESIRED

```
    PRUNE DESIRED
    RPF SGRPT XG EQUAL
  Upstream State: PRUNED
    Local interface list:
    Pruned interface list:
    Outgoing interface list:
      gigabitethernet0/0/3
```

#PC1 can only receive the multicast service packet with multicast group FF10::1 sent by Multicast Server. PC2 can only receive the multicast service packet with multicast group FF50::1 sent by Multicast Server.

Note

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.
- By default, the device enables the SPT switching.

7.10.3 MLD snooping Typical Configuration Example

7.10.3.1 Configure MLD snooping

Network Requirements

- Device1 configures the IPv6 multicast route protocol; Device2 enables MLD 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

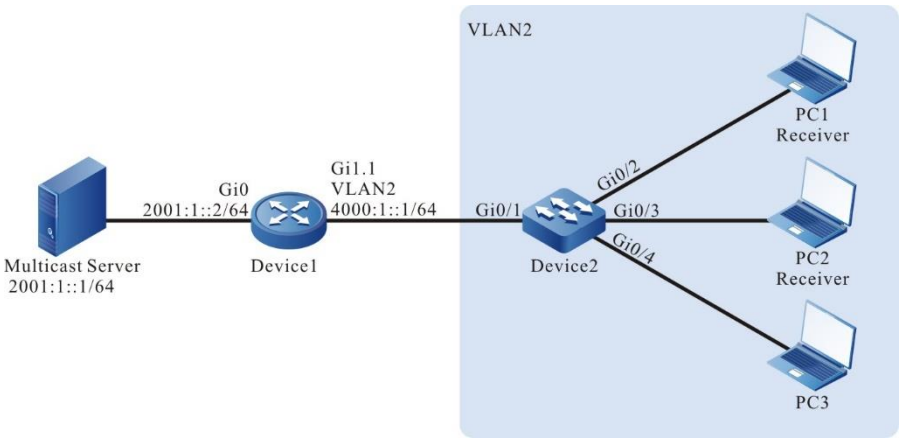


Figure 200 Networking of configuring MLD snooping

Configuration Steps

Step 1: Device1 configure the interface IPv6 address and enables the IPv6 multicast route protocol. (omitted)

Step 2: Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#On Device2, configure the link type of ports gigabitethernet0/2~gigabitethernet0/4 as Access, and permit 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
```

#On Device2, configure the link type of port gigabitethernet0/1 as Trunk, and permit 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
```

#In VLAN2, enable unknown multicast dropping.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l2-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable MLD snooping, and enable the routing port dynamic learning function of VLAN2.

```
Device2(config)#ipv6 mld snooping
Device2(config)#ipv6 mld snooping vlan 2
Device2(config)#ipv6 mld snooping vlan 2 mrouter-learning
```

Step 3: Check the result.

#PC1 and PC2 send MLDv1 member report packet to add IPv6 multicast group FF10::1.

#Query the multicast member table of Device2.

```
Device2#show ipv6 mld snooping groups
MLD Snooping Group Membership
Total 2 groups

VLAN ID  Port Name  Group Address  Expires   Last Reporter   V1 Expires  Uptime
-------  ---------  -------------  --------  ---------  ----------  ---------
2        gi0/2      ff10::1        00:03:59  fe80::b        stopped     00:00:16
2        gi0/3      ff10::1        00:03:59  fe80::c        stopped     00:00:16
```

#Multicast Server sends the IPv6 multicast packet whose destination address is FF10::1, PC2 and PC2 can receive the multicast service packet, and PC3 cannot receive the multicast service packet.

7.11 IPv6 PIM-SM

7.11.1 Overview

IPv6 PIM protocol and IPv4 PIM protocol have the same behaviors except the IP address structure in the packet. Refer to the brief introduction of PIM-SM.

7.11.2 IPv6 PIM-SM Function Configuration

Table 990 IPv6 PIM-SM function configuration list

Configuration Task	
Configure the IPv6 PIM-SM basic functions	Enable the IPv6 PIM-SM protocol

Configuration Task	
Configure the IPv6 PIM-SM aggregation router	Configure C-RP
	Configure static RP
Configure the IPv6 PIM-SM bootstrap router	Configure C-BSR
	Configure the BSR edge
Configure IPv6 PIM-SM multicast source registration	Configure the RP reachability check
	Configure the sending rate of the register packets
	Configure sending rate of the register stop packets
	Configure the source address of the register packet
	Configure register packet filter
Configure IPv6 PIM-SM neighbor parameters	Configure the period of sending the Hello packets
	Configure the keepalive time of the neighbor
	Configure the neighbor filter
	Configure the DR priority
Configure IPv6 PIM-SM SPT switching	Configure the SPT switching condition
Configure IPv6 PIM-SSM	Configure IPv6 PIM-SSM

7.11.2.1 Configure IPv6 PIM-SM Basic Functions

Configuration Conditions

Before configuring IPv6 PIM-SM, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable

Enable IPv6 PIM-SM Protocol

Table 991 Enable the IPv6 PIM-SM protocol

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the IPv6 multicast forwarding	ipv6 multicast-routing	Mandatory By default, the IPv6 multicast forwarding is not enabled.
Enter interface configuration mode	interface *interface-name*	-
Enable the IPv6 PIM-SM protocol	ipv6 pim sparse-mode ipv6 pim sparse-mode passive	Either By default, IPv6 PIM-SM is disabled on the interface.

Note

- After enabling the IPv6 PIM-SM function, all IPv6 PIM-SM configurations can take effect.

7.11.2.2 Configure IPv6 PIM-SM Aggregation Router

Configuration Condition

Before configuring RP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol

Configure C-RP

RP is generated by the C-RP election. After BSR is elected, all C-RPs (Candidate-

Rendezvous Point) regularly unicast the C-RP packet to BSR. BSR integrates the C-RP information and transmits the information to all devices in the IPv6 PIM-SM domain via the bootstrap packet.

Table 992 Configure C-RP

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure C-RP	ipv6 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*]	Mandatory By default, there is no C-RP.

Note

- RP election rules:
- For the group range of the C-RP service, perform the longest matching of the mask.
- If the longest matching of the mask has multiple C-RPs, compare the C-RP priority. The smaller the value, the high the priority. The one with highest priority wins.
- If there are multiple C-RPs with highest priority, perform the HASH calculation for the C-RP address and group. The one with the largest HASH value wins.
- If there are multiple RPs with the largest HASH, the C-RP with the largest IPv6 address wins.

Configure Static RP

For the simple IPv6 PIM-SM network, it is suggested to use the static RP. If using

the static RP, do not need to perform the BSR configuration, eliminating the frequent interacting between RP and BSR, so as to save the network bandwidth.

Table 993 Configure static RP

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the static RP	ipv6 pim rp-address *ipv6-address* [*access-list-name* | *access-list-number*] [override] [vrf *vrf-name*]	Mandatory By default, there is no static RP.

Note

- All devices in the same IPv6 PIM-SM domain should be configured with the same static RP.

7.11.2.3 Configure IPv6 PIM-SM Bootstrap Router

Configuration Conditions

Before configuring BSR, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol

Configure C-BSR

In one IPv6 PIM-SM domain, there should be the unique BSR. Multiple C-BSRs (Candidate-Bootstrap Router) elects to generate the unique BSR via the bootstrap packet.

Table 994 Configure C-BSR

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure C-BSR	ipv6 pim bsr-candidate *interface_name* [*hash-mask-length* [*priority-value*]] [vrf *vrf-name*]	Mandatory By default, there is no C-BSR.

Note

- BSR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IPv6 address wins.

Configure BSR Border

BSR is responsible for collecting the C-RP information and transmits the information to all devices in the IPv6 PIM-SM domain via the bootstrap packet. The BSR range is the range of the multicast domain. The bootstrap packet cannot pass the interface configured with the BSR border. The devices out of the multicast domain range cannot take part in the forwarding of the multicast service packet in the multicast domain, so as to realize the dividing of the multicast domain.

Table 995 Configure the BSR border

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the BSR border	ipv6 pim bsr-border	Mandatory By default, there is no multicast border.

7.11.2.4 Configure IPv6 PIM-SM Multicast Source Register

Configuration Condition

Before configuring the multicast source register, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol

Configure RP Reachability Check

Before source DR sends the register packet to RP, first perform the RP reachability check. If finding that the RP route is not reachable, do not register to RP, so as to reduce the cost of the DR.

Table 996 Configure the RP reachability check

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the RP reachability check	ipv6 pim register-rp-reachability [vrf *vrf-name*]	Mandatory By default, before performing the PIM register, do not check the RP reachability.

Note

- To reduce the cost of the source DR, it is suggested to configure the command on the source DRs of all IPv6 PIM-SMs.

Configure Sending Rate of Register Packets

When the source DR receives the multicast packet, encapsulate the multicast packet to the register packet and send to RP for source register until the registration is complete..

When the source DR does not complete the multicast source register and the multicast flow is large, generate lots of register packets, which increase the load of the RP device. Even RP cannot work normally. Source DR does not need to transmit all register packets of one flow to RP, so configuring the rate of sending the register packets at the source DR not only can reach the purpose of source registration, but also can reduce the RP load.

Table 997 Configure the rate of sending the register packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the rate of sending the register packet	ipv6 pim register-rate-limit *rate-limit-value* [vrf *vrf-name*]	Mandatory By default, do not limit the rate of sending the register packet.

Note

- To reduce the RP load, it is suggested to configure the rate of sending the source register packets on all source DRs.

Configure Sending Rate of Register Stop Packets

After RP receives the register packet of the source DR, send the register stop packet to the source DR to complete the registration. When the RP receives lots of register packets, it is necessary to reply all register packets (send register stop packet).

In fact, there are lots of repeated packets in the register stop packets. You can limit the rate of sending the register stop packet on RP to reduce the cost of RP.

Table 998 Configure the rate of sending the register stop packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the rate of sending the register stop packet	ipv6 pim register-stop-rate-limit *rate-limit-value* [vrf *vrf-name*]	Mandatory By default, do not limit the rate of sending the register stop packet.

Note

- To improve the robustness of the whole IPv6 PIM-SM network, it is suggested to limit the rate of the source register stop packet on all RPs.

Configure Source Address of Register Packet

When the source DR performs the source register, the source address of the register packet uses the IPv6 address of the register interface automatically registered by the system. The command can specify the source address of the register packet as the IPv6 address of one interface on the device to meet some special demand of the network.

Table 999 Configure the source address of the register packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the source address of the register	ipv6 pim register-source interface *interface-name* [vrf *vrf-name*]	Mandatory By default, use IPv6

Step	Command	Description
packet		address of the register interface automatically registered by the system as the source address of the register packet.

Configure Register Packet Filter

To prevent the source register attack, you can use ACL on RP to perform the multicast source filter for the register packet. Only the multicast source permitted by ACL can register successfully on RP.

Table 1000 Configure the register packet filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the register packet filter	ipv6 pim accept-register list { *access-list-number* | *access-list-name* } [vrf *vrf-name*]	Mandatory By default, do not filter the register packet.

7.11.2.5 Configure IPv6 PIM-SM Neighbor Parameters

Configuration Condition

Before configuring the IPv6 PIM-SM neighbor parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol

Configure Sending Period of Hello Packets

The interface enabled with the IPv6 PIM-SM protocol periodically sends the Hello packets to set up and maintain the PIM neighbor.

Table 1001 Configure the period of sending the Hello packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the period of sending the Hello packet	ipv6 pim hello-interval *interval-value*	Optional By default, the period of sending the Hello packet is 30s.

Configure Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 1002 Configure IPv6 PIM-SM neighbor keepalive time

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure IPv6 PIM-SM neighbor keepalive time	ipv6 pim hello-holdtime *holdtime-value*	Optional By default, the keepalive time of the IPv6 PIM-SM neighbor is 105s.

Configure Neighbor Filter

If there are many PIM neighbors in one subnet, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 1003 Configure the neighbor filter

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the neighbor filter	ipv6 pim neighbor-filter { *access-list-number* | *access-list-name* }	Mandatory By default, do not enable the neighbor filter function.

Configure DR Priority

DR plays one important role in the IPv6 PIM-SM network, so selecting the appropriate DR is important. You can select the appropriate device as DR by configuring the DR priority.

One IPv6 PIM-SM subnet only permits one DR. According to the function, DR can be divided to source DR and receiving DR.

The main function of the source DR is to perform the source register to RP.

The main function of the receiving DR is to add to RP and set up the switching of RPT and SPT.

Table 1004 Configure the DR priority

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter interface configuration mode	interface *interface-name*	-
Configure the DR priority	ipv6 pim dr-priority *priority-value*	Optional By default, the DR priority is 1.

Note

- DR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IPv6 address wins.

7.11.2.6 Configure IPv6 PIM-SM SPT Switching

Configuration Condition

Before configuring SPT, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol

Configure SPT Switching Condition

The receiving end DR does not know the address of the multicast source, so it can only add to RP to form RPT. The source DR performs the source register to RP and form the source tree between source DR and RP. At first, the direction of the multicast flow is from multicast source to RP and then from RP to the receiver. When the receiving end DR receives the first multicast packet, it performs adding to multicast source, forms SPT, and performs the pruning for RPT. This is called SPT switching.

The command is to configure the SPT switching condition at the receiving end DR.

Table 1005 Configure the SPT switching condition

Step	Command	Description
Enter global configuration	configure terminal	-

Step	Command	Description
mode		
Configure the SPT switching condition	ipv6 pim spt-threshold { infinity | *threshold* [group-list {*access-list-number* | *access-list-name* }] [vrf *vrf-name*]	Mandatory By default, all multicast groups perform the SPT switching.

Caution

- Do not configure SPT never-switching on RP. Otherwise, it may result in the failure of the multicast forwarding.

7.11.2.7 Configure IPv6 PIM-SSM

IPv6 PIM-SSM is one subset of IPv6 PIM-SM. In IPv6 PIM-SSM, do not need RP, BSR or RPT, and there is no SPT switching, but the receiving end DR directly adds to multicast source and sets up the shortest path tree (SPT) with source as root.

Configuration Condition

Before configuring IPv6 PIM-SSM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, making the intra-domain route reachable
- Enable the IPv6 PIM-SM protocol on all interfaces that need multicast route forwarding

Configure IPv6 PIM-SSM

Table 1006 Configure IPv6 PIM-SSM

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure PIM-SSM	ipv6 pim ssm { default | range { *access-list-number* | *access-list-name* } } [vrf *vrf-name*]	Mandatory By default, the SSM function is disabled.

Caution

- When using IPv6 PIM-SSM, the receiving end should enable MLDv2.
- When the receiver cannot be upgraded to MLDv2, you can use the IGMP SSM Mapping function to cooperate with IPv6 PIM-SSM.
- Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent. Otherwise, it may result in the abnormality of IPv6 PIM-SS.

7.11.2.8 IPv6 PIM-SM Monitoring and Maintaining

Table 1007 IPv6 PIM-SM monitoring and maintaining

Command	Description
clear ipv6 pim bsr rp-set [vrf *vrf-name*]	Clear the RP set information of IPv6 PIM-SM
clear ipv6 pim mroute [*group-address* [*source-address*]] [vrf *vrf-name*]	Clear the multicast route information of IPv6 PIM-SM
clear ipv6 pim statistics [[interface *interface-name* | [vrf *vrf-name*]	Clear the statics information of the IPv6 PIM-SM protocol packets
show ipv6 pim bsr-router [vrf *vrf-name*]	Display the IPv6 PIM-SM bootstrap route information
show ipv6 pim interface [*interface-name* detail | detail] [vrf *vrf-name*]	Display the IPv6 PIM-SM interface information
show ipv6 pim local-members *interface-name* [	Display the IPv6 PIM-SM local group member

Command	Description
vrf *vrf-name*]	information
show ipv6 pim mroute [| ssm | group *group-address* [source *source-address*] | source *source-address*] [vrf *vrf-name*]	Display the IPv6 PIM-SM multicast route table information
show ipv6 pim neighbor [detail] [vrf *vrf-name*]	Display the IPv6 PIM-SM neighbor information
show ipv6 pim nexthop [*ipv6-address*] [vrf *vrf-name*]	Display the IPv6 PIM-SM next-hop router information
show ipv6 pim rp mapping [vrf *vrf-name*]	Display the IPv6 PIM-SM RP information
show ipv6 pim rp-hash *group-address* [vrf *vrf-name*]	Display the RP information of the multicast group mapping
show ipv6 pim statistics [vrf *vrf-name*]	Display the statistics information of the IPv6 PIM-SM protocol packets

7.11.3 IPv6 PIM-SM Typical Configuration Example

7.11.3.1 Configure IPv6 PIM-SM Basic Functions

Network Requirements

- The whole network runs the IPv6 PIM-SSM protocol.
- PC1 and PC2 are the two receivers of Device3 stub network.
- Device1 and Device2 are C-BSR and C-RP.
- Run MLDv2 between Device3 and the stub network.

Network Topology

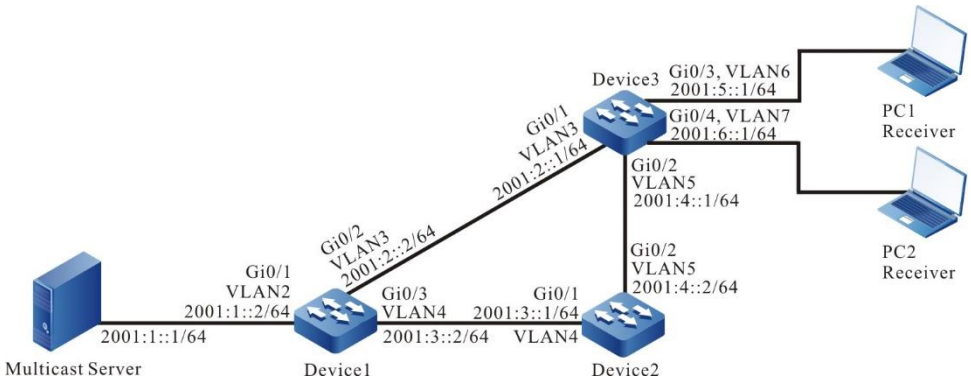


Figure 201 Networking of configuring IPv6 PIM-SM basic functions

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface. (omitted)

Step 3: Enable unicast routing protocol OSPFv3 so that all devices in the network can communicate with each other.

#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 vlan4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf 100 area 0
Device2(config-if-vlan5)#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 vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 router ospf 100 area 0
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 router ospf 100 area 0
Device3(config-if-vlan7)#exit
```

#Query the route 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 ::, 2w6d:04:39:46, lo0
O    2001:1::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
C    2001:2::/64 [0/0]
     via ::, 00:01:05, vlan3
L    2001:2::1/128 [0/0]
     via ::, 00:01:04, lo0
O    2001:3::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
                 [110/2]
     via fe80::201:7aff:fec0:525a, 00:00:04, vlan5
C    2001:4::/64 [0/0]
```

```
    via ::, 00:00:49, vlan5
L   2001:4::1/128 [0/0]
    via ::, 00:00:48, lo0
C   2001:5::/64 [0/0]
    via ::, 00:00:43, vlan6
L   2001:5::1/128 [0/0]
    via ::, 00:00:42, lo0
C   2001:6::/64 [0/0]
    via ::, 00:00:43, vlan7
L   2001:6::1/128 [0/0]
    via ::, 00:00:42, lo0
```

Note

- The query methods of Device1 and Device2 are the same as that of Device3, so the query process is omitted.

Step 4: Globally enable IPv6 multicast forwarding, and enable the multicast protocol IPv6 PIM-SM on the interface.

#Configure Device1.

Globally enable IPv6 multicast forwarding, and enable the multicast protocol IPv6 PIM-SM on the related interface.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding, and enable the multicast protocol IPv6 PIM-SM on the related interface.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
Device2(config-if-vlan5)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding, and enable the multicast protocol IPv6 PIM-SM on the related interface.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 pim sparse-mode
Device3(config-if-vlan7)#exit
```

#Query the information about the interface enabled with the IPv6 PIM-SM protocol on Device3, and IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 5 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF   Nbr   DR   BSR   CISCO   Neighbor
               Index Mode  Flag  Count Pri  Border Neighbor Filter
register_vif0  2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

vlan3          1     v2/S  UP    1     1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d   Global Address: 2001:2::1      DR: fe80::201:7aff:fe62:bb7e
```

```
vlan5          3     v2/S   UP    1     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e    Global Address: 2001:4::1       DR: fe80::201:7aff:fec0:525a

vlan6          4     v2/S   UP    0     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f    Global Address: 2001:5::1       DR: fe80::201:7aff:fe5e:6d2f

vlan7          5     v2/S   UP    0     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d30    Global Address: 2001:6::1       DR: fe80::201:7aff:fe5e:6d30

Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor              Interface      Uptime/Expires     Ver   DR
Address                                                       Priority/Mode
fe80::201:7aff:fe62:bb7e vlan3         00:04:01/00:01:29   v2    1 / DR
fe80::201:7aff:fec0:525a vlan5         00:04:03/00:01:39   v2    1 / DR
```

Note

- The query methods of Device1 and Device2 is the same as that of Device3, and the querying process is omitted.

Step 5: On vlan6 and vlan7 of Device3, enable MLD.

#Configure Device3.

On vlan6 and vlan7 of Device3, enable MLD.

```
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 mld enable
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan7
Device3(config-if-vlan7)#ipv6 mld enable
Device3(config-if-vlan7)#exit
```

#Query the MLD information of interface vlan6 and vlan7 on Device3.

```
Device3#show ipv6 mld interface
Interface vlan6 (Index 11)
```

```
  MLD Enabled, Active
  Querier: fe80::201:7aff:fe5e:6d2f (Self)
  Default version: 2
  Querier parameter:
    Query interval is 125 seconds
    Querier timeout is 255 seconds
    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
    Robustness variable is 2
Interface vlan7 (Index 12)
  MLD Enabled, Active
  Querier: fe80::201:7aff:fe5e:6d30 (Self)
  Default version: 2
  Querier parameter:
    Query interval is 125 seconds
    Querier timeout is 255 seconds
    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
    Robustness variable is 2
```

Note

- You can configure the MLD version running on the interface via the **ip v6 mld version** command.

Step 6: Configure the interface vlan3 of Device1 as C-BSR and C-RP, and configure the interface vlan4 of Device2 as C-BSR and C-RP.

#Configure Device1.

Configure interface vlan3 of Device1 as C-BSR and C-RP, the priority of C-BSR is 200, and the multicast group range of the C-RP service is FF10::/16.

```
Device1(config)#ipv6 pim bsr-candidate vlan3 10 200
Device1(config)#ipv6 access-list extended 7001
```

```
Device1(config-v6-list)#permit ipv6 any ff10::/16
Device1(config-v6-list)#commit
Device1(config-v6-list)#exit
Device1(config)#ipv6 pim rp-candidate vlan3 group-list 7001
```

#Configure Device2.

Configure interface vlan4 of Device2 as C-BSR and C-RP, the priority of C-BSR is 0, and the multicast group range of the C-RP service is FF00::/8.

```
Device2(config)#ipv6 pim bsr-candidate vlan4
Device2(config)#ipv6 pim rp-candidate vlan4
```

#Query the BSR and RP information of Device3.

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:2::2
  BSR Priority: 200
  Hash mask length: 10
  Up time: 00:03:04
  Expiry time: 00:02:06
  Role: Non-candidate BSR
  State: Accept Preferred
Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): ff00::/8
  RP count: 1
    RP: 2001:3::1
      Info source: 2001:2::2, via bootstrap, priority 192
      Up time: 00:21:30
      Expiry time: 00:02:24

  Group(s): ff10::/16
  RP count: 1
    RP: 2001:2::2
      Info source: 2001:2::2, via bootstrap, priority 192
      Up time: 00:04:31
      Expiry time: 00:02:24
```

Note

- The query methods of Device1 and Device2 are the same as that of Device3, and the query process is omitted.
- When configuring multiple C-BSRs in a multicast domain, BSR will be selected first according to priority, and the C-BSR with the highest priority will be selected as BSR. When the priorities of C-BSRs are the same, the C-BSR with the largest IP address is selected as BSR.
- When multiple C-RPs are configured in a multicast domain and the multicast group range of the service is the same, the corresponding RP of multicast group G will be calculated according to the hash algorithm.
- In the multicast domain, you can configure RP by the command **ipv6 pim rp-address**, but the static RP addresses configured on all devices of the entire multicast domain are required to be consistent.

Step 7: Check the result.

#PC1 and PC2 respectively send MLDv2 member relation report to add to multicast group FF10::1 and FF50::1.

#Multicast Server sends the multicast service packet of multicast group FF10::1, FF50::1.

#Query the multicast member table on Device3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group    Interface       Uptime    Expires  V1-Expires   Last Reporter
ff10::1  vlan6           00:00:09  00:04:13 not used     fe80::210:94ff:fe00:1
ff50::1  vlan7           00:00:09  00:04:14 not used     fe80::210:94ff:fe00:2
```

#Query the RP of multicast group FF10::1, FF50::1 on Device3.

```
Device3#show ipv6 pim rp-hash ff10::1
  PIM6 VRF Name: Default
  RP: 2001:2::2
    Info source: 2001:2::2, via bootstrap
Device3#show ipv6 pim rp-hash ff50::1
  PIM6 VRF Name: Default
  RP: 2001:3::1
    Info source: 2001:2::2, via bootstrap
```

#Query the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 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


(*, ff10::1)
Up time: 00:00:06
RP: 2001:2::2
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    vlan6
  Joined interface list:
  Asserted interface list:


(2001:1::1, ff10::1)
Up time: 00:00:05
KAT time: 00:03:25
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
```

Joined interface list:
Asserted interface list:
Outgoing interface list:
vlan6
Packet count 0

(2001:1::1, ff10::1, rpt)
Up time: 00:00:05
RP: 2001:2::2
Flags:
RPT JOIN DESIRED
RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:

(*, ff50::1)
Up time: 00:00:06
RP: 2001:3::1
RPF nbr: fe80::201:7aff:fec0:525a
RPF idx: vlan5
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
vlan7
Joined interface list:
Asserted interface list:

(2001:1::1, ff50::1)
Up time: 00:00:05
KAT time: 00:03:27
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
SPT bit: TRUE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
Joined interface list:
Asserted interface list:
Outgoing interface list:
vlan7
Packet count 1

```
(2001:1::1, ff50::1, rpt)
Up time: 00:00:05
RP: 2001:3::1
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    vlan7
```

#PC1 can only receive multicast service packets sent by Multicast Server, whose multicast group is FF10::1. PC2 can only receive multicast service packets sent by Multicast Server, whose multicast group is FF50::1.

Note

- The query methods of Device1 and Device2 are the same as that of Device3, so the query method is omitted.
- By default, the device enables the SPT switching.

7.11.3.2 Configure IPv6 PIM-SSM

Network Requirements

- The whole network runs the IPv6 PIM-SSM protocol.
- PC is one receiver of Device3 stub network.
- Run MLDv2 between Device3 and the stub network.

Network Topology

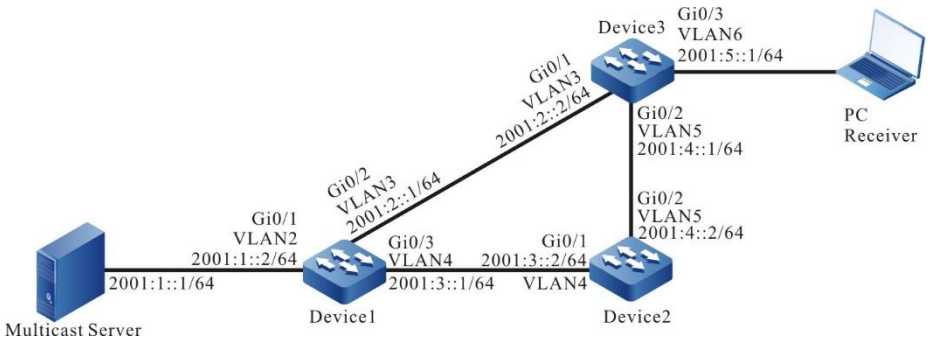


Figure 202 Networking of configuring IPv6 PIM-SSM

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface. (omitted)

Step 3: Enable the unicast route protocol OSPFv3 so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 1 00
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 vlan4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 router ospf 100 area 0
Device2(config-if-vlan5)#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 vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config0)#interface vlan5
Device3(config-if-vlan5)#ipv6 router ospf 100 area 0
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
```

#View the route 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 ::, 2w6d:04:39:46, lo0
O    2001:1::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
C    2001:2::/64 [0/0]
     via ::, 00:01:05, vlan3
L    2001:2::2/128 [0/0]
     via ::, 00:01:04, lo0
O    2001:3::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan3
                [110/2]
     via fe80::201:7aff:fec0:525a, 00:00:04, vlan5
C    2001:4::/64 [0/0]
     via ::, 00:00:49, vlan5
L    2001:4::1/128 [0/0]
     via ::, 00:00:48, lo0
C    2001:5::/64 [0/0]
```

```
    via ::, 00:00:43, vlan6
L   2001:5::1/128 [0/0]
    via ::, 00:00:42, lo0
```

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 4: Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan4
Device2(config-if-vlan4)#ipv6 pim sparse-mode
Device2(config-if-vlan4)#exit
Device2(config)#interface vlan5
Device2(config-if-vlan5)#ipv6 pim sparse-mode
Device2(config-if-vlan5)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 pim sparse-mode
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan5
Device3(config-if-vlan5)#ipv6 pim sparse-mode
Device3(config-if-vlan5)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
```

#View the information of the interface enabled with the IPv6 PIM-SM protocol on Device3 and the IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF  Nbr   DR   BSR   CISCO   Neighbor
               Index  Mode  Flag  Count  Pri  Border Neighbor Filter
register_vif0   2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

vlan3          1     v2/S  UP   1     1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d   Global Address: 2001:2::2      DR: fe80::201:7aff:fe62:bb7e

vlan5          3     v2/S  UP   1     1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e   Global Address: 2001:4::1      DR: fe80::201:7aff:fec0:525a

vlan6          4     v2/S  UP   0     1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f   Global Address: 2001:5::1      DR: fe80::201:7aff:fe5e:6d2f
Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor           Interface      Uptime/Expires     Ver   DR
```

```
Address                                 Priority/Mode
fe80::201:7aff:fe62:bb7e vlan3          00:04:01/00:01:29   v2    1 / DR
fe80::201:7aff:fec0:525a vlan5          00:04:03/00:01:39   v2    1 / DR
```

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 5: Enable MLD on gigabitethernet0/0/2 of Device3.

#Configure Device3.

Enable MLD on vlan6 of Device3.

```
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 mld enable
Device3(config-if-vlan6)#exit
```

#View the MLD information of Device3 interface vlan6.

```
Device3#show ipv6 mld interface vlan6
Interface vlan6 (Index 11)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d2f (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  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
  Robustness variable is 2
```

Note

- You can configure the MLD version running on the interface via ipv6

mld version.

Step 6: Configure IPv6 PIM-SSM on all devices; the multicast group range of the SSM service is FF3X::/32.

#Configure Device1.

```
Device1(config)#ipv6 pim ssm default
```

#Configure Device2.

```
Device2(config)#ipv6 pim ssm default
```

#Configure Device3.

```
Device3(config)#ipv6 pim ssm default
```

Step 7: Check the result.

#PC sends the MLDv2 member relation report of the specified source group to add to multicast group FF30::1; the specified multicast source is 2001:1::1.

#Multicast Server sends the multicast packets with multicast group FF30::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups detail
MLD Connected Group Membership
Total 1 Connected Groups
Group         Interface         Uptime     Expires    V1-Expires Last Reporter
ff30::1       vlan6             00:26:42   not used   not used   fe80::210:94ff:fe00:1
 Group mode : Include
 TIB-A Count: 1
 TIB-B Count: 0

 TIB-A
 Source list: (R - Remote, M - SSM Mapping)
 Source                          Uptime     Expires  Flags
 2001:1::1                       00:05:55   00:03:41 R
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
```

```
PIM6 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


(2001:1::1, ff30::1)
Up time: 00:06:48
KAT time: 00:02:30
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: vlan3
SPT bit: TRUE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  vlan6
 Joined interface list:
 Asserted interface list:
 Outgoing interface list:
  vlan6
 Packet count 275560
```

#PC can only receive the multicast service packet with multicast group FF30::1 sent by Source.

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- The default multicast group range of IPv6 PIM-SSM is FF3X::/32. You can modify the multicast group range of the IPv6 PIM-SSM service via the command ipv6 pim ssm range.
- For the multicast group G meeting the SSM condition, the multicast route table does not generate the (*,G) entry, but just generate the (S,G) entry.

7.11.3.3 Configure IPv6 PIM-SM Multicast Forwarding Control

Network Requirements

- The whole network runs the IPv6 PIM-SM protocol.
- Receiver is one receiver of Device3 stub network.
- Device2 is C-BSR and C-RP.
- On Device2 and Device3, control for the multicast source, making PC only receive the multicast service packet sent by Multicast Server 1.
- Run MLDv2 between Device3 and the stub network.

Network Topology

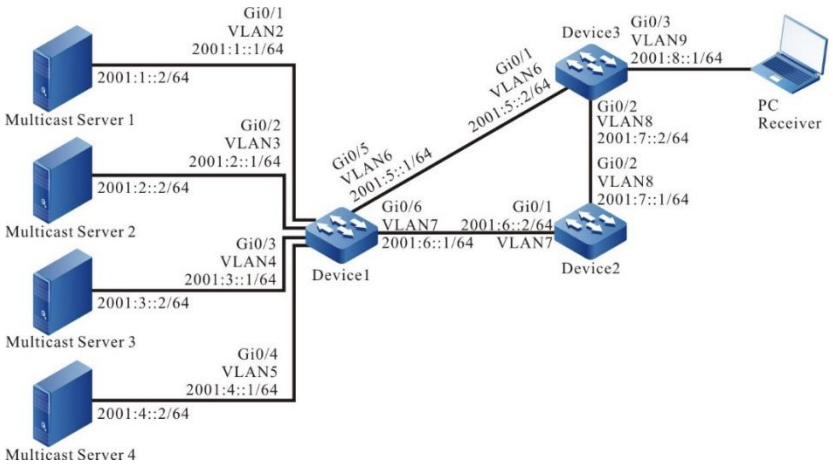


Figure 203 Networking of configuring IPv6 PIM-SM multicast forwarding control

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface. (omitted)

Step 3: Enable the unicast route protocol OSPFv3 so that all devices in the

network can communicate with each other.

#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
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 router ospf 100 area 0
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ipv6 router ospf 100 area 0
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ipv6 router ospf 100 area 0
Device1(config-if-vlan7)#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 vlan7
Device2(config-if-vlan7)#ipv6 router ospf 100 area 0
Device2(config-if-vlan7)#exit
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ipv6 router ospf 100 area 0
Device2(config-if-vlan8)#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 vlan6
```

```
Device3(config-if-vlan6)#ipv6 router ospf 100 area 0
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ipv6 router ospf 100 area 0
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 router ospf 100 area 0
Device3(config-if-vlan9)#exit
```

#View the route 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 ::, 3w2d:05:13:23, lo0
O    2001:1::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O    2001:2::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O    2001:3::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
O    2001:4::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
C    2001:5::/64 [0/0]
     via ::, 00:01:52, vlan6
L    2001:5::2/128 [0/0]
     via ::, 00:01:50, lo0
O    2001:6::/64 [110/2]
     via fe80::201:7aff:fe62:bb7e, 00:00:24, vlan6
           [110/2]
     via fe80::201:7aff:fec0:525a, 00:00:24, vlan8
C    2001:7::/64 [0/0]
     via ::, 00:01:25, vlan8
L    2001:7::2/128 [0/0]
     via ::, 00:01:24, lo0
C    2001:8::/64 [0/0]
     via ::, 00:01:16, vlan9
L    2001:8::1/128 [0/0]
     via ::, 00:01:14, lo0
```

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 4: Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 pim sparse-mode
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 pim sparse-mode
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 pim sparse-mode
Device1(config-if-vlan4)#exit
Device1(config)#interface vlan5
Device1(config-if-vlan5)#ipv6 pim sparse-mode
Device1(config-if-vlan5)#exit
Device1(config)#interface vlan6
Device1(config-if-vlan6)#ipv6 pim sparse-mode
Device1(config-if-vlan6)#exit
Device1(config)#interface vlan7
Device1(config-if-vlan7)#ipv6 pim sparse-mode
Device1(config-if-vlan7)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface vlan7
Device2(config-if-vlan7)#ipv6 pim sparse-mode
Device2(config-if-vlan7)#exit
```

```
Device2(config)#interface vlan8
Device2(config-if-vlan8)#ipv6 pim sparse-mode
Device2(config-if-vlan8)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol IPv6 PIM-SM on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 pim sparse-mode
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ipv6 pim sparse-mode
Device3(config-if-vlan8)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 pim sparse-mode
Device3(config-if-vlan9)#exit
```

#View the information of the interface enabled with the IPv6 PIM-SM protocol on Device3 and the IPv6 PIM-SM neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF   Nbr   DR    BSR   CISCO   Neighbor
               Index Mode  Flag  Count Pri   Border Neighbor Filter
register_vif0  2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

vlan6          1     v2/S  UP    1     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d   Global Address: 2001:5::2      DR: fe80::201:7aff:fe62:bb7e

vlan8          4     v2/S  UP    1     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e   Global Address: 2001:7::2      DR: fe80::201:7aff:fec0:525a

vlan9          3     v2/S  UP    0     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f   Global Address: 2001:8::1      DR: fe80::201:7aff:fe5e:6d2f
Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
```

```
Total 2 Neighbor entries

Neighbor                Interface      Uptime/Expires     Ver   DR
Address                                                         Priority/Mode
fe80::201:7aff:fe62:bb7e vlan6         00:07:08/00:01:25  v2    1 / DR
fe80::201:7aff:fec0:525a vlan8         00:00:18/00:01:27  v2    1 / DR
```

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 5: Configure gigabitethernet0/0/0 of Device2 as the C-BSR and C-RP of the whole network and the multicast group range of the C-RP service is FF00::/8.

#Configure Device2.

```
Device2(config)#ipv6 pim bsr-candidate vlan7
Device2(config)#ipv6 pim rp-candidate vlan7
```

#View the BSR and RP information of Device3.

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:6::2
  BSR Priority: 0
  Hash mask length: 126
  Up time: 00:00:21
  Expiry time: 00:01:54
  Role: Non-candidate BSR
State: Accept Preferred

Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): ff00::/8
```

```
RP count: 1
  RP: 2001:6::2
    Info source: 2001:6::2, via bootstrap, priority 192
    Up time: 00:00:28
    Expiry time: 00:02:02
```

Note

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

Step 6: On Device2 and Device3, control for the multicast source, making PC only receive the multicast service packet sent by Multicast Server 1.

#On Device2, configure the accepted register message access list, filtering the register message of Multicast Server 4.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#deny ipv6 host 2001:4::2 any
Device2(config-std-nacl)#permit ipv6 any any
Device2(config-std-nacl)#commit
Device2(config-std-nacl)#exit
Device2(config)#ipv6 pim accept-register list 7001
```

#On interface valn6 and vlan8 of Device3, configure the ingress IPv6 acl, filtering the multicast service packets of Multicast Server 3.

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#deny ipv6 host 2001:3::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#interface vlan6
Device3(config-if-vlan6)#ipv6 access-group 7001 in
Device3(config-if-vlan6)#exit
Device3(config)#interface vlan8
Device3(config-if-vlan8)#ipv6 access-group 7001 in
Device3(config-if-vlan8)#exit
```

#On interface vlan9 of Device3, configure the ingress IPv6 acl, filtering the

multicast service packets of Multicast Server 2.

```
Device3(config)#ipv6 access-list extended 7002
Device3(config-v6-list)#deny ipv6 host 2001:2::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#commit
Device3(config-v6-list)#exit
Device3(config)#interface vlan9
Device3(config-if-vlan9)#ipv6 access-group 7002 out
Device3(config-if-vlan9)#exit
```

Step 7: Check the result.

#PC sends the MLDv2 member relation report to add to multicast group FF10::1.

Multicast Server 1, Multicast Server 2, Multicast Server 3, and Multicast Server 4 all send the multicast packets of multicast group FF10::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group    Interface          Uptime    Expires   V1-Expires  Last Reporter
ff10::1  vlan9              00:35:31  00:03:31  not used    fe80::210:94ff:fe00:1
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 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

(*, ff10::1)
Up time: 00:04:25
RP: 2001:6::2
RPF nbr: fe80::201:7aff:fec0:525a
RPF idx: vlan8
Flags:
  JOIN DESIRED
Upstream State: JOINED
```

Local interface list:
vlan9
Joined interface list:
Asserted interface list:

(2001:1::2, ff10::1)
Up time: 00:03:33
KAT time: 00:01:51
RPF nbr: fe80::201:7aff:fe62:bb7e
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 159075

(2001:1::2, ff10::1, rpt)
Up time: 00:03:33
RP: 2001:6::2
Flags:
RPT JOIN DESIRED
PRUNE DESIRED
RPF SGRPT XG EQUAL
Upstream State: PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:
vlan9

(2001:2::2, ff10::1)
Up time: 00:03:33
KAT time: 00:01:51
RPF nbr: fe80::201:7aff:fe62:bb7e
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 156062

(2001:2::2, ff10::1, rpt)
Up time: 00:03:33
RP: 2001:6::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

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

#View the matching of IPv6 ACL on Device2.

```
Device2#show ipv6 access-list 7001
ipv6 access-list extended 7001
 10 deny ipv6 host 2001:4::2 any     14 matches
 20 permit ipv6 any any     51 matches
```

#View the matching of IPv6 ACL on Device3.

```
Device3#show ipv6 access-list 7001
ipv6 access-list extended 7001
 10 deny ipv6 host 2001:3::2 any     10760 matches
 20 permit ipv6 any any     4089685 matches

Device3#show ipv6 access-list 7002
ipv6 access-list extended 7002
 10 deny ipv6 host 2001:2::2 any     2046914 matches
 20 permit ipv6 any any     2049595 matches
```

#PC end can only receive the multicast service packets sent by Multicast Server 1.

Caution

- When performing the multicast source control, you'd better first configure the multicast source control and then on-demand multicast source, because by default, after receiving the multicast service packet, the receiving end DR performs the SPT switching. If first on-demanding multicast source and then performing the multicast forwarding control, the multicast forwarding control does not take function. To prevent the multicast forwarding control from not taking function, you can configure not permitting SPT switching on the receiving end DR.

8 QoS

8.1 Hardware QoS

8.1.1 Overview

8.1.1.1 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.

8.1.1.2 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.

8.1.1.3 Introduction to QoS Functions

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 four kinds of priority mapping: map the packet DSCP to the local priority (LP); map the 802.1p priority of the packet to the local priority (LP); 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. The diagram of the priority mapping relation is as follows:

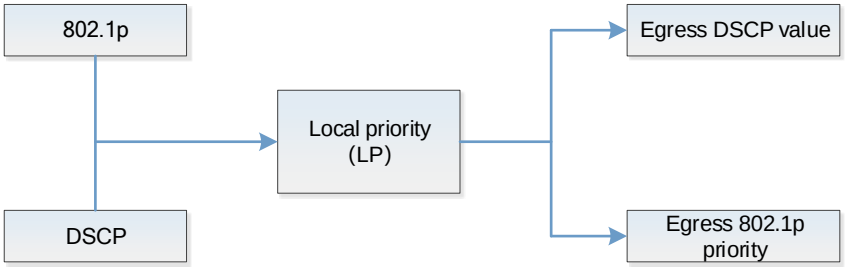


Figure 204 Diagram of priority mapping relation

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.

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), 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.

WDRR (Weighted Deficit Round Robin): 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:

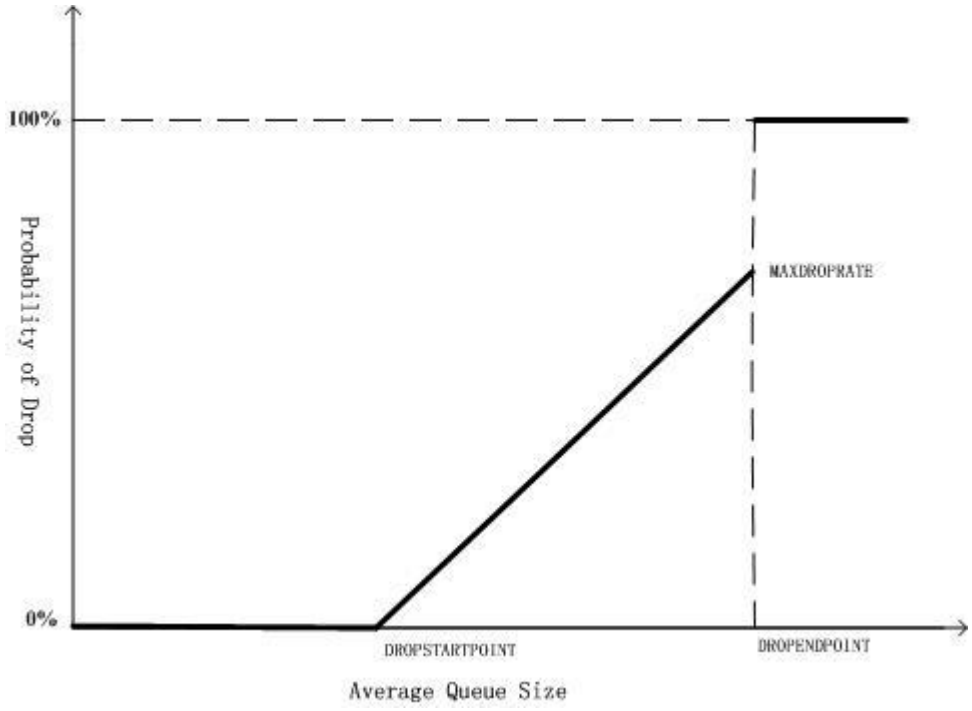


Figure 205 WRED diagram

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.

8.1.2 Hardware QoS Function Configuration

Table 1008 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 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
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

Configuration task	
	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 the priority-based traffic control	Configure the priority-based traffic control
Display the explicit congestion notification	Display the explicit congestion notification

8.1.2.1 Configure Priority Mapping

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 1009 Configure the priority mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the priority mapping profile	qos map-table {ingress | egress } *template-name*	Mandatory Configure the egress and ingress priority profile.

Step	Command	Description
Enter the profile view	{ dot1p-lp | dscp-lp | lp- dot1p | lp-dscp } *index* to *value*	Optional By default, the priority mapping in the profile is the default mapping relation.
Bind the port with the priority mapping profile	map-table *template- name* { ingress | egress }	Mandatory By default, do not bind the priority mapping profile.

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-Ip mapping and dotlp-lp are configured in the profile at the same time. The dscp-lp has higher priority and it takes effect first.
- After enabling the ingress dot1p-lp mapping, the 802.1p priority of the forwarded packet is not 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 still 1.
- 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.

- If the QINQ function is enabled on the port, and the bound profile of the port contains dot1p-lp and dscp-lp mappings, maybe you cannot get the desired mapping result. Therefore, it is recommended not to enable the port binding priority mapping function of QINQ on one port at the same time.
- After configuring the lp-dscp mapping, the default mapping of lp-dscp is 0 to 0, 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 1010 Configure the default priority mapping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the priority mapping profile	qos map-table {ingress | egress } *template-name*	Mandatory Configure the ingress and egress priority profile.
Configure the default priority mapping	{ dot1p-lp | dscp-lp | lp- dot1p | lp-dscp } default *value*	Mandatory By default, do not configure the default priority mapping.

Configure Priority Trust

Priority trust is divided into the ingress trust and egress trust of the interface. The ingress trust can be mapped to local priority (LP) according to 802.1p priority or DSCP value in the packet; The egress trust is to modify 802.1p priority or DSCP value

according to local priority (LP).

By default, the packet priority of the interface trust is the ingress 802.1p priority.

Table 1011 Configure the priority trust of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the priority mapping profile	qos map-table trust {dot1p | dscp} {ingress | egress}	Mandatory By default, configure the ingress dot1p trust.

8.1.2.2 Configure 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.

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 1012 Configure the counter

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the L3 action group	l3-action-group *l3-action-*	Either

Step	Command	Description
and enter the L3 action group configuration mode	*group-name*	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. After entering the PBR action group configuration mode, subsequent configurations are only effective in the current PBR 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 PBR action group and enter the PBR action group configuration mode	pbr-action-group *pbr-action-group-name*	
Configure the counter	count { all-colors }	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 and yellow according to the packet traffic, and then the counter will count the number of the packets of different colors.

Table 1013 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 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 yellow and meter mode configuration. An incomplete configuration will not take effect.
Configure the meter actions	meter action yellow { drop | transmit }	Optional By default, the packets in 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
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*	

Step	Command	Description
		group configuration mode, the subsequent configuration just takes effect in the current egress action group
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 lp or remark dotlp-lp action.
- You cannot re-mark the yellow packet.
- 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 mirror the matched packet to the specified port or session.

Table 1014 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 By default, the flow mirror is not configured.
	mirror session *sessionId*	Mandatory 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.

Table 1015 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* |interface link-aggregation *link-aggregation-id*}	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 1016 Configure re-marking l2-priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the L3 action group	l3-action-group *l3-action-*	Either

Step	Command	Description
and enter the L3 action group configuration mode	*group-name*	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 { dscp *dscp-value* |{{ dot1p | dot1p-lp | lp } { *priority-value* | precedence }}}	Mandatory By default, re-marking l2-priority is not configured.

Note

- In the action group, the priority field in the TOS of IP packet cannot be used to retag the 802.1p priority in the VLAN tag.
- The egress action group does not support the remark action.

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 1017 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 entering the egress action group configuration mode, the subsequent configuration just takes effect in the current egress action group.
Configure the egress action group and enter the egress action group configuration mode	egr-action-group *egr-action-group-name*	
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.

- In the action group, the 802.1p priority in VLAN Tag cannot be used to retag the priority field in the TOS of the IP packet.
- The egress action group does not support the remark action.

8.1.2.3 Configure Traffic Monitoring

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 1018 Configure port-based rate limitation

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the L2/L3 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.

8.1.2.4 Configure Traffic Shaping

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 1019 Configure queue-based traffic shaping

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure queue-based traffic shaping	traffic-shape queue *queue-id* { { cir *cir* [cbs *cbs*] pir *pir* [pbs *pbs*] } | { cir *cir* [cbs *cbs*]} | { pir *pir* [pbs *pbs*] } }	Mandatory By default, queue-based traffic shaping is not configured.

Step	Command	Description

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 1020 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{ {pir *rate* [pbs *burst-size*] } | { *priority* pir *rate* [pbs *burst-size*][time-range *range-name*] } }	Mandatory By default, port-based traffic shaping is not configured.

Configure Port-based Traffic Policer Shaping

Port-based traffic shaping allows the binding of time domain to achieve the purpose of shaping different time periods into different bandwidths. Each port can be configured with eight traffic shaping with different priorities. Each traffic shaping can be bound to the time domain. The entries that take effect at the same time are determined by the priority level. The priority level is 0, the highest and 7, the lowest.

Table 1021 Configure the port-based traffic policer shaping

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 port-based traffic policer shaping	traffic-policer { {pir *rate* pbs *burst-size* } | { *priority* pir *rate* pbs *burst-size*[time-range *range-name*] } }	Mandatory By default, do not configure port-based traffic shaping.

8.1.2.5 Configure Congestion Management

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), 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.

WDRR (Weighted Deficit Round Robin): 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 1022 Configure the scheduling policy for the port queue

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Configure the scheduling policy for the port queue	queue-schedule { sp | rr | {{ wdrr|wrr } *weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7*}}	Mandatory By default, the scheduling policy for the port queue is the SP.

8.1.2.6 Configure Congestion Avoidance

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 1023 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.

8.1.2.7 Configure VFP Action Group

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 1024 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 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 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 1025 Configure the processing for the packet with double-layer VLAN tag

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
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 1026 Configure the processing for the packet without 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 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 1027 Configure binding VRF in the VFP action group

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
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.

8.1.2.8 Hardware QoS Monitoring and Maintaining

Table 1028 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
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 user-name [*template name* {ingress | egress}]	Display the priority mapping profile information
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-vlan-range | inst-interface-vlan-range | { inst-interface *interface-name* | inst-interface-vlan *vlan-id* | inst-link-aggregation *link-aggregation-id* | inst-vlan *vlan-id* } { ip-in | ip-out | ipv6-in | ipv6-out | mac-in | mac-out | hybrid-in | hybrid-out }}	Display the counter information of the ACL applied to the specified object
show traffic-meter [*traffic-meter-name*]	Display all counter information

Command	Description
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 ecn	Display whether ECN is enabled on the device
show priority-flow-control [*interface interface-name*]	Display the flow control configuration of all priorities on the port

8.1.3 Typical Configuration Example of Hardware QoS

8.1.3.1 Configure Priority Mapping

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

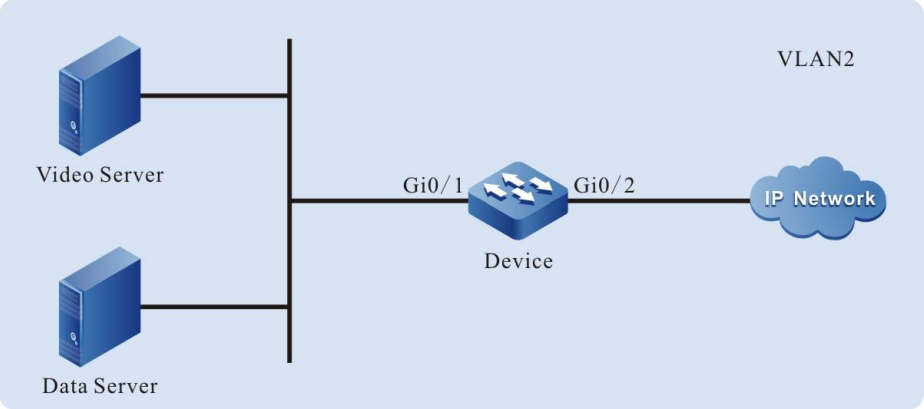


Figure 206 Networking of configuring the priority mapping

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 globally, map the packet with DSCP value 34 to queue 2 and map the packet with DSCP value 38 to queue 3.

```
Device(config)#qos map-table ingress a
Device(config-maptable-ingress)#dscp-lp 34 to 2
Device(config-maptable-ingress)# dscp-lp 38 to 3
```

#Globally configure the priority mapping function, 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)#qos map-table egress b
Device(config-maptable-egress)#lp-dot1p 2 to 5
Device(config- maptable-egress)# lp-dot1p 3 to 1
```

#Bind the profile and configure trust on the port.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)# map-table a ingress
Device(config-if-gigabitethernet0/1)#qos map-table trust dscp ingress
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# map-table b egress
Device(config-if-gigabitethernet0/2)#qos map-table trust dot1p egress
```

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.

8.1.3.2 Configure Remarking

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

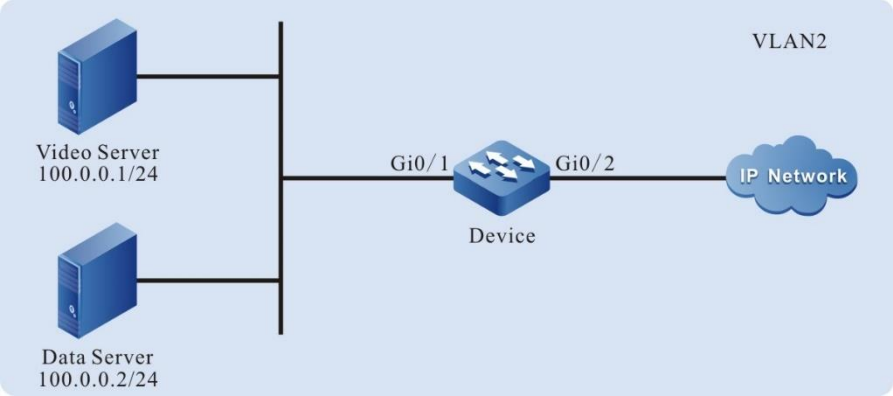


Figure 207 Networking of configuring the remarking

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)#commit
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.

8.1.3.3 Configure Traffic Shaping

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

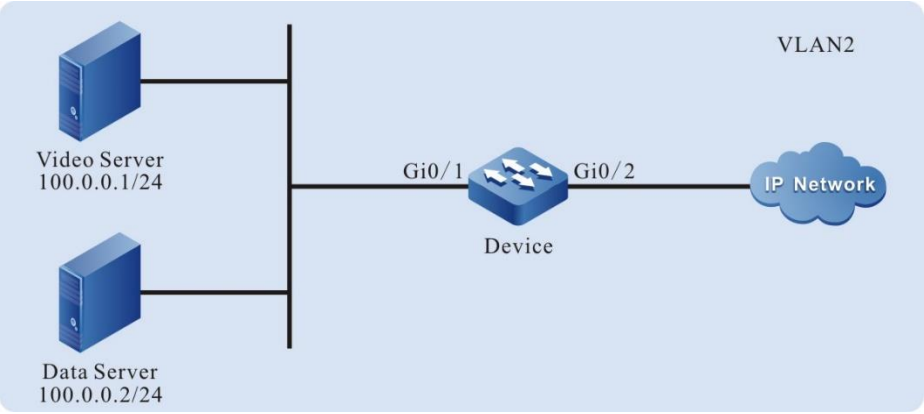


Figure 208 Networking of configuring the traffic shaping

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)#commit
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 cir 20000 cbs 4096 pir 20000 pbs 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 pir 50000 pbs 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.

8.1.3.4 Configure Rate Limitation

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

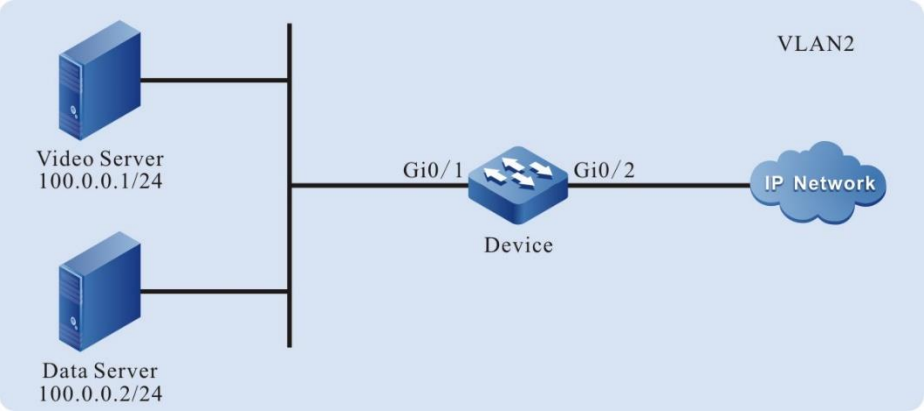


Figure 209 Networking of configuring the rate limitation

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)#commit
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.

8.1.3.5 Configure WRED

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

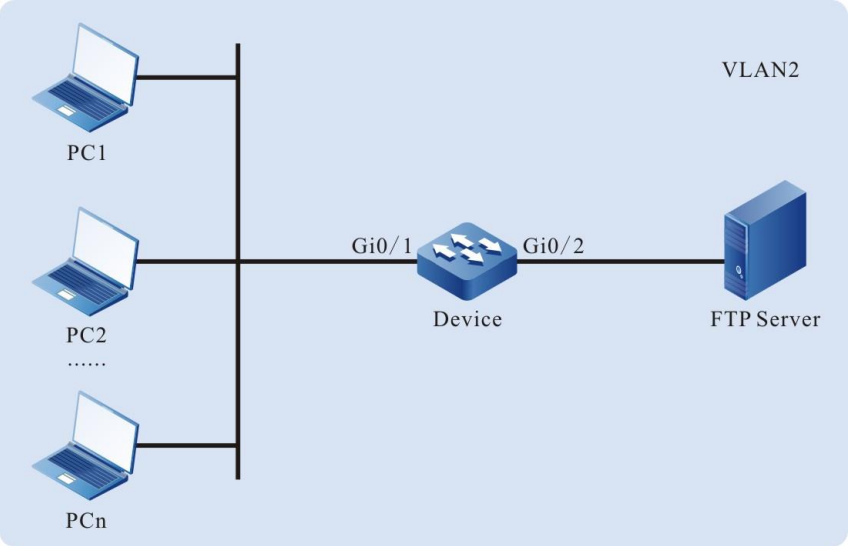


Figure 210 Networking of configuring WRED

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.

8.1.3.6 Configure SP

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

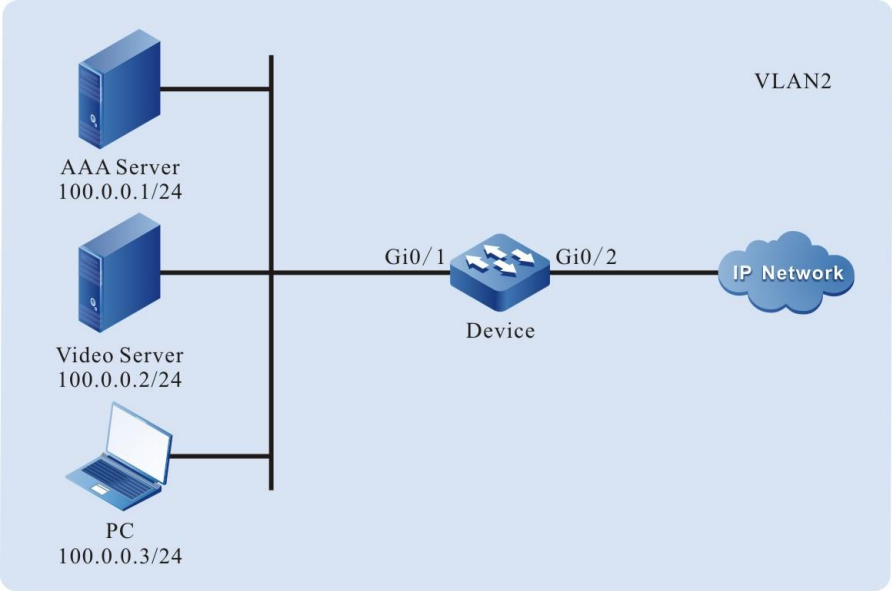


Figure 211 Networking of configuring the SP

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)#commit
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.

8.1.3.7 Configure WDRR

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

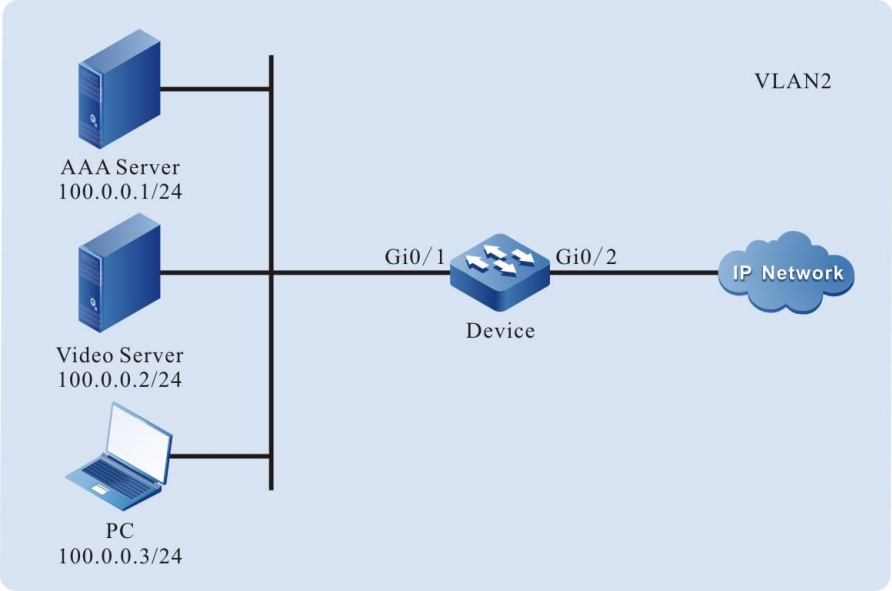


Figure 212 Networking of configuring the WDRR

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)#commit
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, the terminal traffic, video traffic and authentication traffic pass by the proportion of 1:2:3.

8.1.3.8 Configure SP+WDRR

Network Requirements

- There is authentication server (AAA Server), video server and one terminal device (PC) in the network.
- Configure the SP+WDRR 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

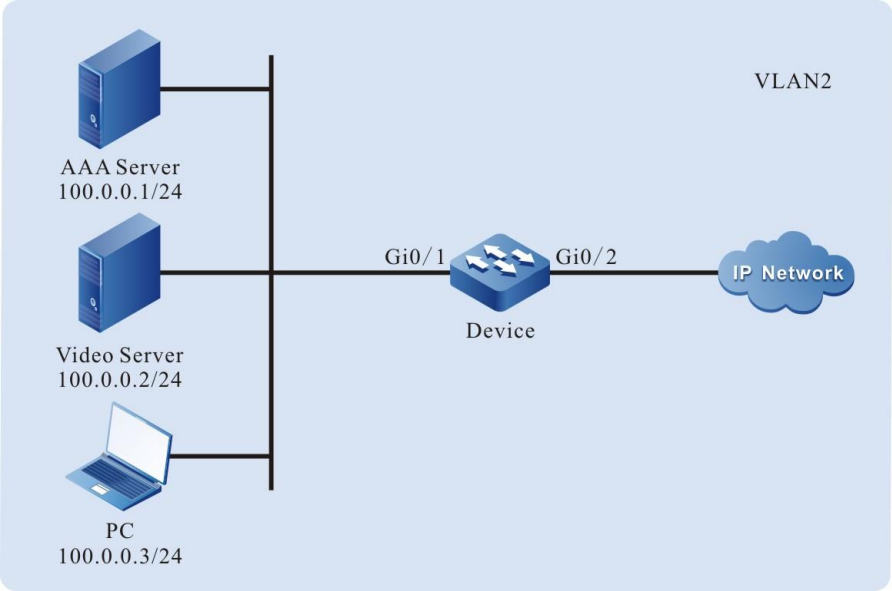


Figure 213Networking of configuring the SP+WDRR

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)#commit
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 + WDRR function.

#Configure the SP+WDRR 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.

8.1.3.9 Configure Flow Mirror

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

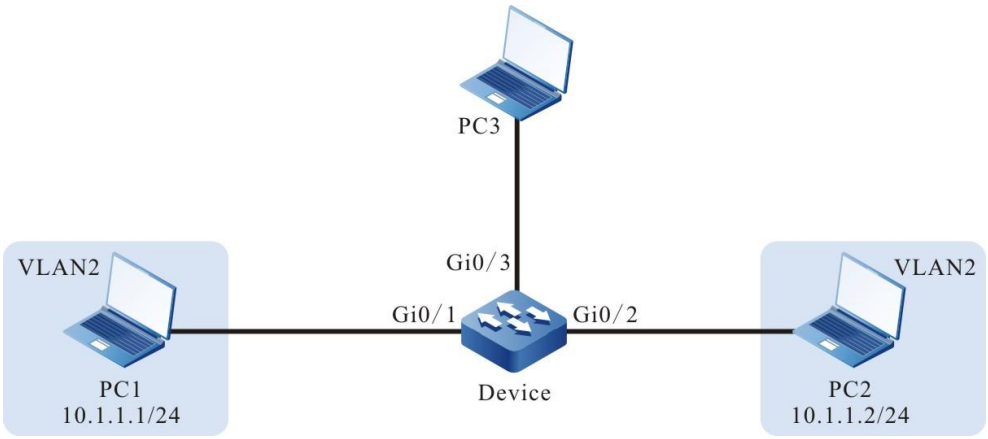


Figure 214 Networking of configuring the flow mirror

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 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)#commit
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
```

Step 5: Check the result.

#When PC1 and PC2 communicate with each other, we can capture the packets received by port gigabitethernet0/1 on PC3.

9 Security

9.1 ARP Check

9.1.1 Overview

ARP Check is one function of checking the validity of the ARP packet, preventing the invalid ARP packet from passing and improving the network security.

The validity check of the ARP packet is based on the port binding entry. The binding entry includes two types:

Static binding entry: Manual configured static binding entry;

Dynamic binding entry: Dynamically generated by the valid entry of the DHCP Snooping function and 802.1X function.

The checking principle of ARP Check is as follows:

In the ARP packet received by the port, check the sending IP address, source MAC address to match the port ARP Check binding entry. If matching, the ARP packet is valid packet and is forwarded directly. Otherwise, the ARP packet is invalid packet and is dropped.

9.1.2 ARP Check Function Configuration

Table 1029 ARP Check function configuration list

Configuration Task	
Enable the port ARP Check function	Enable the port ARP Check function
Bind the ARP Check static entry	Bind the ARP Check static entry
Re-install the entry that does not succeed in writing the hardware	Re-install the entry that does not succeed in writing the hardware

9.1.2.1 Enable Port ARP Check Function

Configuration Condition

None

Enable Port ARP Check Function

After enabling the ARP Check function of the port, ARP Check dynamically gets the entry in the DHCP Snooping database and writes the ACL hardware.

Table 1030 Enable the port ARP Check 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	interface link-aggregation *link-aggregation-id*	
Enable the ARP Check function of the port	arp-check enable	Mandatory By default, the port ARP Check function is not enabled.

9.1.2.2 Bind ARP Check Static Entry

Configuration Condition

None

Bind ARP Check Static Entry

Table 1031 Bind ARP Check static entry

Step	Command	Description
Enter global configuration mode	config terminal	-
Enter the L2 Ethernet interface configuration	interface *interface-name*	Either

Step	Command	Description
mode		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	interface link-aggregation *link-aggregation-id*	
Bind the ARP Check static entry	arp-check binding *mac-address ip-address* [rate *limit-value*]	Mandatory By default, do not configure the ARP Check static binding entry

9.1.2.3 Re-install ARP Check Entry Not Succeeded in Writing Hardware

Configuration Condition

None

Re-install ARP Check Entry Not Succeeded in Writing Hardware

Table 1032 Re-install ARP Check Entry Not Succeeded in Writing Hardware

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
Enter the aggregation group	interface link-	

Step	Command	Description
configuration mode	aggregation *link-aggregation-id*	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.
Re-install ARP Check entry not succeeded in writing hardware	arp-check install	Mandatory By default, do not install ARP Check entry not succeeded in writing hardware

9.1.2.4 ARP Check Monitoring and Maintaining

Table 1033 ARP Check monitoring and maintaining

Command	Description
show arp-check [active | brief | inactive | interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Display the information in the ARP Check entry

9.1.3 ARP Check Typical Configuration Example

9.1.3.1 Configure Basic Functions of ARP Check

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the ARP Check basic function, realizing that PC1 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

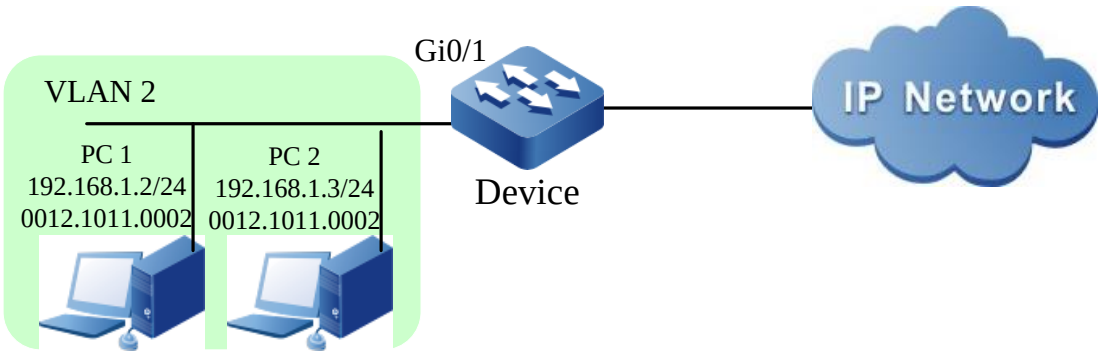


Figure 215 Networking of configuring the ARP Check basic functions

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 the 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
Device(config-if-gigabitethernet0/1)#exit
```

Step 2: Configure the ARP Check function on Device.

#Enable the ARP Check function on the port gigabitethernet0/1 and configure the ARP Check binding entry with MAC address 0012.1011.0002 and IP address 192.168.1.2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#arp-check enable
Device(config-if-gigabitethernet0/1)#arp-check binding 0012.1011.0002 192.168.1.2 rate 10
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

#View the ARP Check configuration information.

Device#show arp-check brief

Interface Name Status Binding Table

---

gi0/1 Enable Yes

You can see that the port gigabitethernet0/1 is enabled with the ARP Check function, and there is the ARP Check entry.

#View the port ARP Check binding entry.

```
Device#show arp-check interface gigabitethernet0/1
-------------------------ARP Check Table-----------------------------------
Interface-Name  Status  MAC-Address  IP-Address  Rate  PolicySource   SetHardware
-------------------------------------------------------------------------------
gi0/1        enable  0012.1011.0002  192.168.1.2  10  STATIC      active
total number: 1
```

#PC1 can access IP Network normally, but PC2 cannot access IP Network.

9.1.3.2 Combine ARP Check with DHCP Snooping

Network Requirements

- PC1 and PC2 are connected to IP Network via Device; PC1 uses the static IP address and PC2 gets the IP address via DHCP.
- Device configures the DHCP Snooping and ARP Check function, realizing that PC2 can access IP Network normally and PC1 cannot access IP Network.

Network Topology

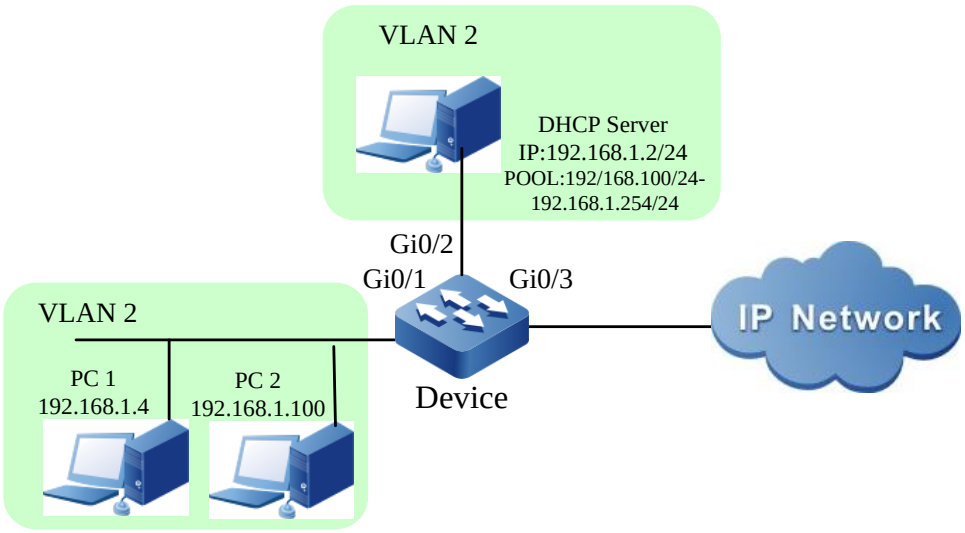


Figure 216 Networking of combining ARP Check with DHCP Snooping

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 the port gigabitethernet0/1, gigabitethernet0/2, and gigabitethernet0/3 as Access, all permitting the services of VLAN2 to pass.

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

Step 2: Configure the DHCP Snooping function on Device.

#Enable the DHCP Snooping function and configure the port gigabitethernet0/2 as trust port.

```
Device(config)#dhcp-snooping
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp-snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure the ARP Check function on Device.

#Enable the ARP Check function on the port gigabitethernet0/1.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#arp-check enable
Device(config-if-gigabitethernet0/1)#exit
```

Step 4: Check the result.

#After PC2 gets the IP address successfully, view the DHCP Snooping dynamic entry on Device.

```
Device#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
    ------
```

#View the ARP Check binding entry of the port gigabitethernet0/1.

```
Device#show arp-check interface gigabitethernet0/1
-------------------------ARP Check Table-----------------------------------
Interface-Name  Status  MAC-Address  IP-Address  Rate  PolicySource   SetHardware
-------------------------------------------------------------------------------
gi0/1        enable  0013.0100.0001 192.168.1.100  15   DHCPSP      active
total number: 1
```

#PC2 can access IP Network normally, but PC1 cannot.

9.1.3.3 Combine ARP Check with 802.1XNetwork Requirements

- PC1 is connected to IP Network via Device, and Device adopts 802.1X access control.
- The authentication mode adopts the RADIUS authentication.
- PC1 cannot access the network if not being authenticated successfully. After passing the authentication, PC1 is permitted to access IP Network.

- The authenticated user can generate the arp-check entry to perform the validity detection for the arp packet of the authenticated user.

Network Topology

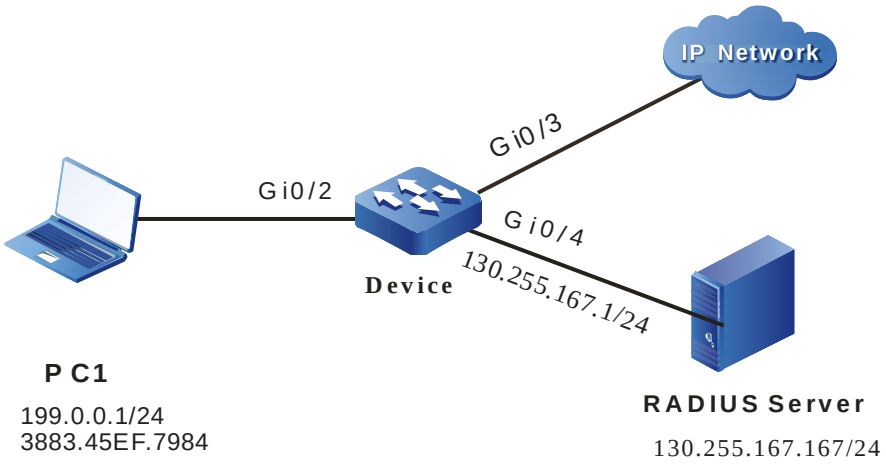


Figure 217 Networking of combining ARP Check with 802.1X

Configuration Steps

Step 1: On Device, configure the link type of the VLAN and port.

#On Device, create VLAN2~VLAN4.

```
Device#configure terminal
Device(config)#vlan 2-4
Device(config)#exit
```

#Configure the link type of port gigabitethernet 0/2 as access, permitting the services of VLAN2 to pass.

Device(config)#interface gigabitethernet 0/2

```
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#On gigabitethernet 0/3-gigabitethernet 0/4 of Device, configure the port link type as Access, permitting the services of VLAN3-VLAN4 to pass respectively (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN4 as 130.255.167.1/24.

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

Step 3: Configure the AAA authentication.

#On Device, enable the AAA authentication, 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)#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 the AAA server.

#On the AAA server, configure the user name, password, and key value as admin (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)#authentication port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: On Device, configure the ARP Check function.

#Enable the ARP Check function on port gigabitethernet0/2.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#arp-check enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 7: Authenticate successfully.

#Before passing authentication, PC1 cannot access the network.

#After initiating the authentication and being authenticated successfully, PC1 can 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=  199.0.0.1
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1    Authorized: 1   Unauthorized/guest/critical: 0/0/0   Unknown: 0
```

Step 8 : Check the result.

```
Device#show arp-check interface gigabitethernet0/2
-------------------------ARP Check Table-----------------------------------
Interface-Name  Status  MAC-Address  IP-Address  Rate  PolicySource   SetHardware
-------------------------------------------------------------------------------
gi0/2         enable   3883.45ef.7984 199.0.0.1  15   DOT1X      active

total number: 1
```

#If the arp packet sent by PC1 matches with the entry completely, forward it and limit the speed normally. If not matching, drop it directly.

9.2 CPU Protection

9.2.1 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.

9.2.2 CPU Protection Function Configuration

Table 1034 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 total rate limitation of all CPU queues
	Configure the rate limitation of each CPU queue
Configure the customized protocol packet to be processed by CPU	Configure the matching rule of the customized protocol packet to be processed by CPU
	Configure the mode of the customized protocol packet to be processed by CPU

9.2.2.1 Configure CPU Queue of Protocol Packets

Configuration Condition

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 1035 Configure the CPU queue of the protocol packet

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.

9.2.2.2 Configure Total Rate Limitation of All CPU Queues

Configuration Condition

None

Configure Total Rate Limitation of All CPU Queues

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 total rate limitation of all CPU queues. If there is attack and the total packet rate in all queues exceeds the total limited rate, the packets are dropped, avoiding causing the too high CPU utilization.

Table 1036 Configure the total rate limitation of all CPU queues

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
Configure the total rate limitation of all CPU queues	cpu-packet cos global pps *pps-value*	Mandatory By default, the total limited rate of all queues is 2000PPS.

9.2.2.3 Configure Rate Limitation of Each CPU Queue

Configuration Condition

None

Configure Rate Limitation of Each 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 1037 Configure the rate limitation of each CPU queue

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the rate limitation of each CPU queue	cpu-packet cos *cos-value* pps *pps-value*	Mandatory By default, the rate limitation of each queue is different.

9.2.2.4 Configure Customized Protocol Packet to Be Processed by CPU

Configuration Condition

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 1038 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-protocol *protocol-type* | vlan-id *vlan-id* [dst-ip *dst-ip-address* | ingress *ingress-interface* | ip-protocol *protocol-type*]] | ipv6 [dst-ip6 *dst-ipv6-address* | dst-mac *dst-mac* | ingress *ingress-interface* | ip-protocol *protocol-type* | vlan-id *vlan-id* [dst-ip *dst-ip-address* | ingress *ingress-interface* | ip-protocol *protocol-type*]] } |	Mandatory By default, there is no any match rule.

Step	Command	Description
	ingress *ingress-interface* | vlan-id *vlan-id* [ingress *ingress-interface*] }	

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 1039 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.

9.2.2.5 Monitoring and Maintaining of CPU Protection

Table 1040 Monitoring and maintaining of the CPU protection

Command	Description
show cpu-packet protocol-config-table	Display the configuration information of all protocol packets sent to CPU
show cpu-packet cos	Display the current and default queue information of the protocol packets to be processed by CPU
show cpu-packet pps	Display the rate limitation information of each CPU queue
show cpu-packet udf-table	Display all customized ACL entry information set via the CPU protection module

9.2.3 Typical Configuration Example of CPU Protection

9.2.3.1 Configure Basic Functions of CPU Protection

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 packet that reaches the local device can first get the CPU processing.
- Perform the rate limitation for the ARP queue on Device so that when the CPU utilization of Device is too high, the packet with low priority can be processed normally.

Network Topology

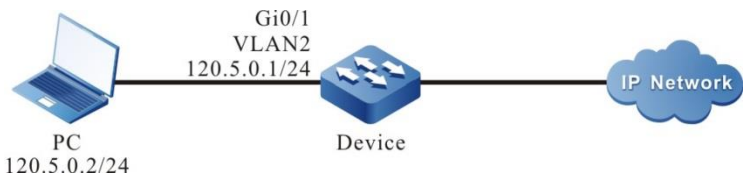


Figure 218 Networking of configuring the CPU protection basic functions

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(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]
ipv6-all              0          [0]
pppoe                 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]
LBD_l2-src-miss       0          [0]
ipaddr-0              0          [0]
ipaddr-127            0          [0]
ipv4-all              0          [0]
src-martian-addr      0          [0]
arp                   1          [1]
ip6-solicited-node    1          [1]
host-group            1          [1]
```

router-group 1 [1]
ND 1 [1]
trill-oam 1 [1]
rarp 1 [1]
lldp 2 [2]
dot1x 2 [2]
dhcp 2 [2]
dhcpv6 2 [2]
http 2 [2]
svi-ip 5 [2]
vxlan 2 [2]
pim 3 [3]
pim6 3 [3]
igmp-dvmrp 3 [3]
ip6-interface-multicast 3 [3]
ike 3 [3]
ntp 3 [3]
mld 3 [3]
rsvp 4 [4]
ospf 4 [4]
ospfv3 4 [4]
irmp 4 [4]
rip 4 [4]
ripng 4 [4]
is-is 4 [4]
bgp 4 [4]
ldp 4 [4]
ipsec-esp 4 [4]
ipsec-ah 4 [4]
mlag-keep-alive 4 [4]
mvst 5 [5]
l2-interface-unicast 5 [5]
gvrp 5 [5]
mvst-inspection 5 [5]
ulfd 5 [5]
l2pt 5 [5]
svi-icmp 5 [5]
ethernet-cfm 5 [5]
ethernet-lmi 5 [5]
mlag-pts 5 [5]
mpls-oam 5 [5]
bfd 6 [6]
vbrp 6 [6]
vrrp 6 [6]
vrrp3 6 [6]

```
telnet                6          [6]
ssh                   6          [6]
loopback-detect       6          [6]
slow-protocols        6          [6]
stp-bpdu              6          [6]
stp-vist              6          [6]
radius-tacacs         6          [6]
trill                 6          [6]
bfdv6-echo            6          [6]
eips                  7          [7]
ulpp                  7          [7]
mad-fast-hello        7          [7]
erps                  7          [7]
mlag                  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]
TOTAL 2000          [2000]
```

You can see that the limited queue 1 rate of ARP on device is modified from the default 250pps to 50pps.

9.2.3.2 Configure Customized Rule of CPU Protection

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

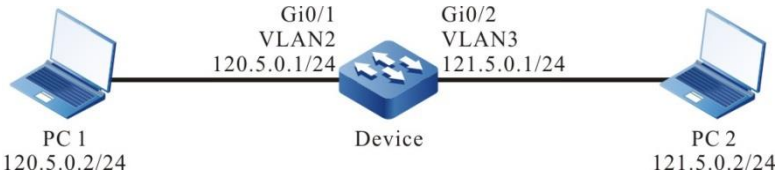


Figure 219 Networking of configuring the customized rule of the CPU protection

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.

9.3 Port Security

9.3.1 Overview

9.3.1.1 Overview of Port Security

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.

9.3.1.2 Port Security Rule

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, MAC+IP binding, and MAC+IPv6 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.

IPv6 rules: Control whether the host can communicate according to the IPv6 address of the host. IPv6 rules can be bound for a single IPv6 address or for IPv6 address segments;

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, IP rule, and IPv6 binding

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, MAC+VLAN binding, MAC+IP binding, and MAC + IPv6 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 and the STICKY learn mode is MAC mode, convert the dynamic MAC entry learned by the MAX rule to the STICKY rule and save in the running configuration.

VOICE VLAN rules: It mainly controls the host's communication according to whether the MAC address of the host belongs to the OUI configured by VOICE-VLAN. These MAC addresses do not include the list of legitimate MAC addresses generated by MAC rules, IP rules and IPv6 binding.

9.3.1.3 Work Principle of Port Security

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. The processing for the IPv6 packet is similar.

9.3.2 Port Security Function Configuration

Table 1041 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 IPv6 rule
	Configure the MAX rule
	Configure the STICKY rule
	Configure the VOICE VLAN rule
Configure the learn mode of the STICKY rule	Configure the learn mode of 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

Configuration Task	
Configure the log sending interval when receiving the invalid packet	Configure the log sending interval when receiving the invalid packet
Configure the port security to use the ACL function	Configure the port security to use the ACL function

9.3.2.1 Configure Basic Functions of Port Security

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 Condition

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 1042 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	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
Enable the port security function	port-security enable	Mandatory By default, the port security function is not enabled.

Note

- The IP rule and MAX rule of the port security and 802.1x cannot be used on one port at the same time.
- The IP rule and MAX rule of the port security and MAC address authentication cannot be used on one port at the same time.
- The port security and secure channel authentication function 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.

9.3.2.2 Configure Port Security Rule

Configuration Condition

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 1043 Configure the MAC rule

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	interface 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*] | ipv6-address *ipv6-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* | ipv6-address *ipv6-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 1044 Configure the 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	interface 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 IPv6 Rule

If hoping to control whether the terminal can communicate via the IPv6 address, the user can use the IPv6 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 1045 Configure the IPv6 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	interface link-aggregation *link-aggregation-id*	
Configure the IPv6 rule whose action is permit	port-security permit ipv6-address *ipv6-address-value* [to *ipv6-address-value*]	Either By default, the IPv6 rule is not configured in the port.
Configure the IPv6 rule whose action is refuse	port-security deny ipv6-address *ipv6-address-value* [to *ipv6-address-value*]	

Note

Port security is the role of security access at data link layer. For the currently supported MAC+IPv6, IPv6 and other rules related to IPv6, once the corresponding effective entry is generated, subsequent packets can be forwarded normally as long as they match the generated MAC + VLAN entry, and IPv6 address is not checked.

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 1046 Configure the 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 configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
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.
Configure the video rule	port-security vedio security enable	Mandatory When the switch is the video mode, the function is enabled by default.
When there is illegal video device is connected, shutdown the port.	port-security vedio security shutdown	When there is the illegal device connected to the video switch, shutdown the port. The function is disabled by default.

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 1047 Configure the 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 just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the MAX rule	port-security maximum *maximum-number*	Mandatory By default, the number of the dynamic MAC

Step	Command	Description
		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*] | ip-address *ip-address-value* [desc *security-rule-description*] | ipv6-address *ipv6-address-value* [desc *security-rule-description*]]]	Mandatory By default, the STICKY rule is not configured in the port.

Configure VOICE VLAN Rule

Under the port that enables the port security function, if the user wants to access the terminal that does not match the MAC rules and IP rules, VOICE-VLAN packets can also communicate, and does not want to be limited by the number of Max rule addresses, voice VLAN rules can be configured, which will allow all packets of OUI configured for VOICE-VLAN to pass through.

Table 1048 Configure the VOICE VLAN 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 VOICE VLAN rule	port-security permit voice vlan	Mandatory By default, the VOICE VLAN rule is not configured in the port.

Note

- The source MAC allowed by the voice VLAN rule is the OUI configured by the source VOICE-VLAN.
- After the max rule is enabled, the voice VLAN rule does not take effect.

Configure Specified Video Rule

In the video switch mode, you can choose to enable or disable the access of Dahua and HIK cameras; or add a device of a specific manufacturer that can access the switch.

Table 1049 Configure the specified video rule

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure Dahua camera	port-security vedio dahua enable	By default, the Dahua camera

Step	Command	Description
		function is enabled.
Configure HIK camera	port-security vedio hikvision enable	By default, the HIK camera function is enabled.
Configure the device of the specified manufacturer to be permitted to access the switch	port-security vedio oui-mac mac-address-*value* mask mac-address-*mask-value*	mac-address-*value* the MAC address of the manufacturer mac-address-*mask-value* the mask of the mac address, get the MAC address information of the specified manufacturer by the mac address and mask information

Note

- The function can be used only in the video switch mode.

9.3.2.3 Configure Learn Mode of STICKY Rule

Configuration Condition

Before configuring the learn mode of the STICKY rule, first complete the following task:

- Enable the port security function

Configure Learn Mode of STICKY Rule

If the user hopes to perform STICKY learning by MAC or MAC + VLAN, you can configure the learn mode of the STICKY rule as MAC mode. If the user hopes to perform the STICKY rule learning by MAC +IP, you can configure the learn mode of the STICKY rule as MAC+IP mode.

Table 1050 Configure the learn mode of the STICKY rule

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	interface link-aggregation *link-aggregation-id*	
Configure the learn mode of the STICKY rule	port-security permit mac-address sticky mode { mac | mac-ip }	Mandatory By default, the learn mode of the STICKY rule is MAC mode.

9.3.2.4 Configure Aging Function of Static MAC Address

Configuration Condition

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 1051 Enable the aging function of the 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	interface 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 1052 Configure the age time of the 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the age time of the static MAC address	port-security aging time *time-value*	Mandatory By default, the age time of the static MAC address is 1 minute.

9.3.2.5 Configure Processing Mode when Receiving Invalid Packet

Configuration Condition

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 1053 Configure the processing mode when receiving the 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	interface link-aggregation *link-aggregation-id*	
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.

9.3.2.6 Configure Log Sending Interval When Receiving Invalid Packet

Configuration Condition

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 1054 Configure the log sending interval when receiving the 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.

9.3.2.7 Configure Port Security to Use ACL Function

Configuration Condition

Before configuring the MAC + IP rule to use the ACL function, first complete the following task:

- Enable the port security function

Configure Port Security to Use ACL

Users can configure whether the port security uses ACL according to actual needs. When using ACL, MAC+IP, MAC+IPv6, STICKY MAC+IP, and STICKY MAC+IPv6 rules can accurately match the source MAC address and source IP/IPv6 address of the user, avoiding illegal user access with source MAC address matching and source IP/IPv6 address mismatching.

Table 1055 Configure MAC+IP rule to use 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
Enter the aggregation group configuration	interface link-	

Step	Command	Description
mode	aggregation *link-aggregation-id*	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 port security to user ACL	port-security use-acl	Mandatory By default, the port security does not use ACL.

9.3.2.8 Monitoring and Maintaining of Port Security

Table 1056 Monitoring and maintaining of the port security

Command	Description
clear port-security statistics	Clear up the statistics information of the sent and received packets
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 ipv6-address	Display the configured IPv6 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
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
show port-security statistics	Display the statistics information of the sent and received packets
show port-security vedio security	In the video switch mode, display the enabling status of the

Command	Description
	video function
show port-security vedio oui	In the video switch mode, display the OUI information supported by the video function by default

9.3.3 Typical Configuration Example of Port Security

9.3.3.1 Configure MAC and IP Rule of Port Security

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

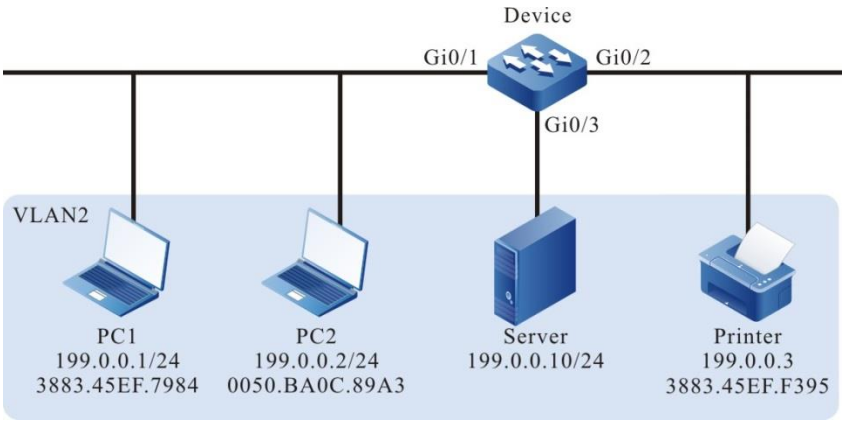


Figure 220 Networking of configuring port security MAC and IP rule

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type 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/IPv6 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.

9.3.3.2 Configure MAC Rule of Port Security

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

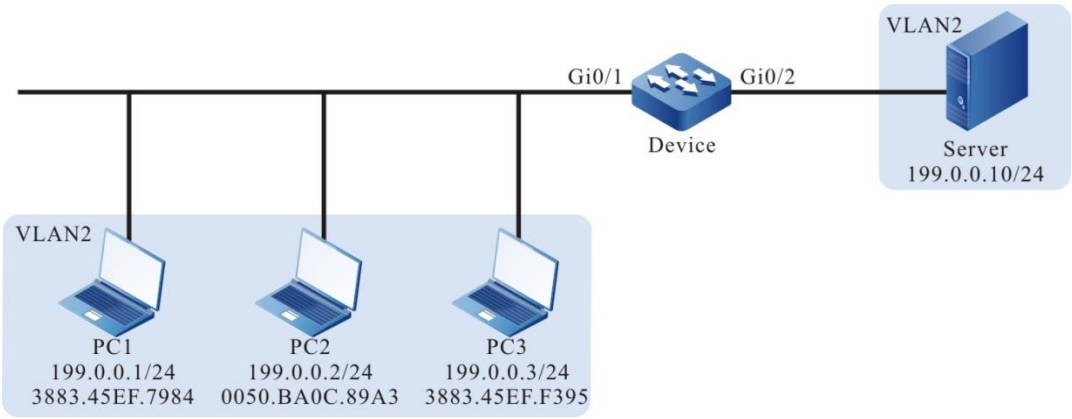


Figure 221 Networking of configuring the MAX rule of the port security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type 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/IPv6 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
```

9.3.3.3 Configure STICKY Rule of Port Security

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

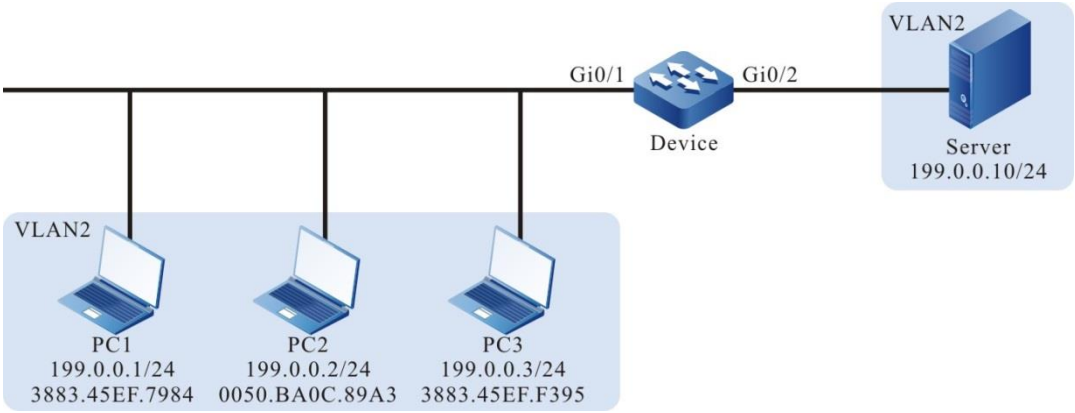


Figure 222 Networking of configuring the STICKY rule of the port security

Configuration Steps

Step 1: Configure VLAN.

#Create VLAN.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the port link type 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/IPv6 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/IPv6 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
```

9.4 IP Source Guard

9.4.1 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, MAC, and IP+MAC. The specific processing modes are as follows:

- IP 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.
- MAC mode: If the source MAC in the packet is the same as the MAC address, VLAN number recorded in the binding table, the port will forward the packet. Otherwise, drop it.
- IP+MAC 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 setting of the filter type takes effect only for the dynamic binding entry, not affecting the static binding entry.

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, or the source MAC address in the IP packet is the same as the MAC address in the global IP Source Guard bound entries, but the source

IP address id 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, or the source MAC address in the ARP packet is the same as the MAC address in the bound entries, but the sending IP address is different, drop the packet.

9.4.2 IP Source Guard Function Configuration

Table 1057 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
	Configure the filter packet type of port IP Source Guard
Configure the global IP Source Guard function	Configure the global IP Source Guard function

9.4.2.1 Configure Static Bound Entries of Port IP Source Guard

Configuration Condition

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, only the static entries configured with mac, ip, and vlan can serve as the basis of the validity detection for the ARP packets.

Table 1058 Configure the 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	interface link-aggregation *link-aggregation-id*	
Configure the static bound entries of the port IP Source Guard	ip source binding { ip-address *ip-address* [mac-address *mac-address* [vlan *vlan-id*] | vlan *vlan-id*] | mac-address *mac-address* [vlan *vlan-id*] }	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.

9.4.2.2 Configure Port IP Source Guard Function

Configuration Condition

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 1059 Configure the 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	interface link-aggregation *link-aggregation-id*	
Enable the port IP Source Guard function	ip verify source	Mandatory By default, the port IP Source Guard function is disabled.

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.

9.4.2.3 Configure Filtered Packet Type of Port IP Source Guard

Configuration Condition

Before configuring the filtered packet type of the port IP Source Guard, first complete the following task:

- Enable the port IP Source Guard function

Configure Filtered Packet Type of Port IP Source Guard

After enabling the port IP Source Guard function, the IP packet is filtered by means of ip. When the source IP address and VLAN number of the IPv4 packet received by the port are the same as the source IP address and VLAN number in the binding entry of the port IP Source Guard, the port forwards the packet; if any one is different, drop the packet.

After enabling the port IP Source Guard function, IP packets are filtered by means of ip-mac. When the source MAC address, source IP address and VLAN number of the IP packet received by the port are the same as the MAC address, IP address and VLAN number in the binding entries of the port IP Source Guard, the port forwards the packet; if any one is different, drop the packet.

After enabling the port IP Source Guard function, IP packets are filtered by means of mac. When the source MAC address and VLAN number of the IP packet received by the port are the same as the MAC address and VLAN number in the binding entries of the port IP Source Guard, the port forwards the packet; if any one is different, drop the packet.

Table 1060Configure the filtered packet type 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	interface link-aggregation *link-aggregation-id*	
Enable the port IP Source Guard	ip verify source type {ip |	Mandatory

Step	Command	Description
function	ip-mac | mac}	By default, the filter mode is IP filter type, taking effect only for the dynamic entry.

9.4.2.4 Configure Static Entry Binding Function of Port MAC

Configuration Condition

None

Configure Static Entry Binding Function of Port MAC

After configuring the port MAC static entry binding function, get the corresponding mac address, vlan number, and port number from the configured IP Source Guard static entries and got dynamic entries on the port, and deliver the corresponding static MAC entry.

Table 1061 Configure the MAC static entry binding 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	interface link-aggregation *link-aggregation-id*	
Enable the port IP Source	ip source sticky-mac	Mandatory

Step	Command	Description
Guard function		By default, the static entry binding function of the port MAC is disabled.

9.4.2.5 Configure Global IP Source Guard Function

Configuration Condition

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 1062 Configure the global IP Source Guard function

Step	Command	Description
Enter global configuration mode	config terminal	-
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

- 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.

9.4.2.6 IP Source Guard Monitoring and Maintaining

Table 1063 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

9.4.3 Typical Configuration Example of IP Source Guard

9.4.3.1 Configure Effective Port IP Source Guard Function Based on DHCP Snooping Dynamic Entries

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure global IP Snooping function.
- Configure the port IP Source Guard function, so that PC2 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

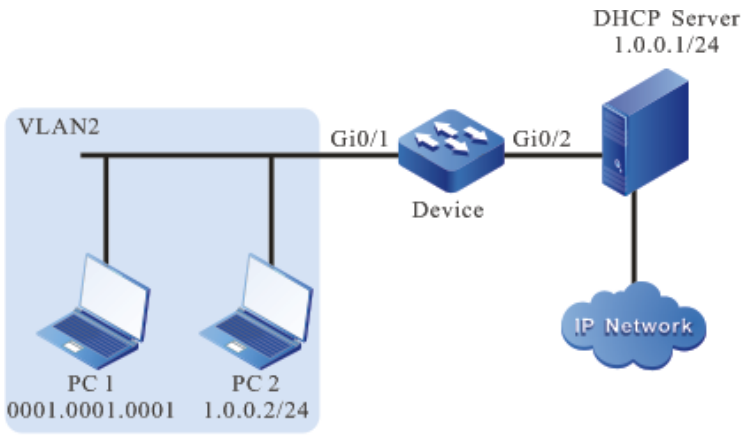


Figure 223 Networking of configuring effective port IP Source Guard function based on DHCP Snooping dynamic entries

Configuration Steps

Step 1: On Device, configure VLAN and port link type.

#Create VLAN2.

```
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: On Device, enable global DHCP Snooping function and configure gigabitethernet0/2 connected to DHCP Server as the trust port.

```
Device(config)#dhcp snooping enable
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dhcp snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure the address pool of DHCP Server as 1.0.0.0/24. (omitted)

Step 4: On Device, configure the IP Source Guard function of the port.

#On port gigabitethernet0/1, enable port-based IP Source Guard function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#exit
```

Step 5: Check the result.

#View the configuration information of DHCP Snooping.

```
Device#show dhcp-snooping
    dhcp-snooping configuration information:
    dhcp-snooping status:enable
    dhcp-snooping option82 information status:disable
    dhcp-snooping option82 information policy:replace
    dhcp-snooping option82 information format:default
    dhcp-snooping option82 information remote id:default(mac address)
    dhcp-snooping information relay-address :None
    dhcp-snooping binding agent save mode :auto-flash
    dhcp-snooping binding agent save delay :1800
    dhcp-snooping binding agent save pool :30
    dhcp-snooping interface information :
    ------------------------------------------------------------
    interface        trust-status    rate-limit(pps)  circuit-Id
    gi0/0/1          untrust         40               default(vlan-mod-interface)
    gi0/0/2          trust           ----             default(vlan-mod-interface)
    gi0/0/3          untrust         40               default(vlan-mod-interface)
    gi0/0/4          untrust         40               default(vlan-mod-interface)
```

```
gi0/0/5          untrust        40          default(vlan-mod-interface)
……
```

#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  L2 Status
-------------------------------------------------------
gi0/1              Enabled        ip        Disabled
gi0/2               Disabled      ip        Disabled
gi0/3               Disabled      ip        Disabled
gi0/4               Disabled      ip        Disabled
gi0/5               Disabled      ip        Disabled
……
```

You can see that port gigabitethernet0/1 is enabled with the IP Source Guard function, and Verify Type is ip. Therefore, in the above example, the dynamic entries take effect based on ip+vlan.

#View the IP Source Guard bound entries of the port.

```
Device#show ip binding table
-------------------------------------------
IP Source Guard binding table on slot 0
   Total binding entries    : 1
   Static binding entries   : 0
   Dynamic binding entries  : 1
   Dynamic not write entries : 0
   PCE writing entries      : 1
-------------------------------------------------------------------------------
----
Interface-Name MAC-Address   IP-Address   VLAN-ID  Type-Flag  Writing-Flag   L2-Flag
-------------------------------------------------------------------------------
----
gi0/1       0001.0001.0001  1.0.0.2     2       dynamic     Write       Not Write
```

#PC1 can access IP Network normally, and PC2 cannot access IP Network.

9.4.3.2 Configure Port IP Source Guard Function Based on Static Entries

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the effective port IP Source Guard function based on static entries, so that PC2 can access IP Network normally and PC2 cannot access IP Network.

Network Topology

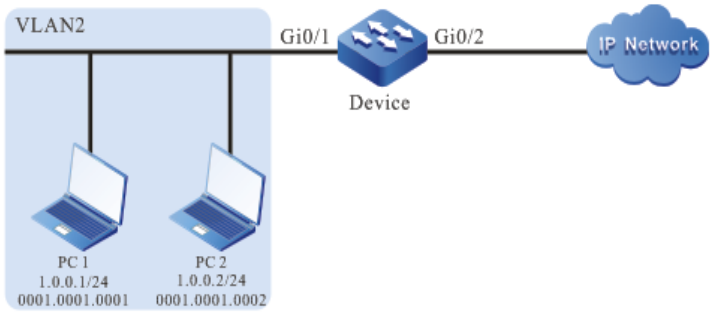


Figure 224 Networking of configuring effective port IP Source Guard function based on static entries

Configuration Steps

Step 1: On Device, configure VLAN and port link type.

Create VLAN2.

```
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: On Device, configure the IP Source Guard function of the port.

#On port gigabitethernet0/1, enable the IP Source Guard function based on MAC+VLAN filtering mode, and configure IP address as 1.0.0.1, and port IP Source Guard binding entries of VLAN2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip verify source
Device(config-if-gigabitethernet0/1)#ip source binding ip-address 1.0.0.1 vlan 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   L2 Status
------------------------------------------------------------
gi0/1              Enabled        IP       Disabled
gi0/2              Disabled       IP       Disabled
gi0/3              Disabled       IP       Disabled
gi0/4              Disabled       IP       Disabled
```

……

You can see that port gigabitethernet0/1 is enabled with the IP Source Guard function. The static IP Source Guard entries take effect according to the configured IP+VLAN entries, not related with the Verify Type value. Therefore, in the above example, the dynamic entries take effect based on ip+vlan.

#View the IP Source Guard bound entries of the port.

```
Device #show ip binding table
----------------------------------------
IP Source Guard binding table on slot 0
   Total binding entries    : 1
   Static binding entries   : 1
   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
-------------------------------------------------------------------------------
----
gi0/1           ---          1.0.0.1     2        Static     Write         Not Write
```

#PC1 can access IP Network normally, and PC2 cannot access IP Network.

9.5 IPv6 Source Guard

9.5.1 Overview

The IPv6 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 IPv6 Source Guard function filters the IPv6 packets received by the specified port. The filter mode includes IP, IP+MAC, and MAC. The specific processing modes are as follows:

- IP mode: If the source IPv6 address and VLAN ID in the packet are the same as the IPv6 address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop it.
- IP+MAC+VLAN mode: If the source IPv6 address, source MAC address, and VLAN ID in the packet are the same as the IPv6 address, MAC address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop the packet.
- MAC+VLAN mode: If the source MAC address, and VLAN ID in the packet are the same as the MAC address and VLAN ID recorded in the bound entries, the port forwards the packet. Otherwise, drop the packet.

The setting of the filter type takes effect only for the dynamic binding entry, not affecting the static binding entry.

The bound entries of the port IPv6 Source Guard include two kinds:

- Static bound entries, manual configured port IPv6 Source Guard static

bound entries

- Dynamic bound entries, dynamically generated by the valid entries of the DHCPv6 Snooping function.

1. Global IPv6 Source Guard function filters the packets received by all ports. The specific filter modes are as follows:

- If the source IPv6 address or MAC address in the IPv6 packet is different from the IPv6 address or source MAC address in the global IPv6 Source Guard bound entries, but the source MAC address is different, drop the packet.

9.5.2 IPv6 Source Guard Function Configuration

Table 1064 The configuration list of the IPv6 Source Guard function

Configuration Tasks	
Configure the basic functions of the port IPv6 Source Guard	Enable the port IPv6 Source Guard function
	Configure the bound entries of the port IPv6 Source Guard
Configure the filtered packet type of the port IPv6 Source Guard	Configure the filtered packet type of the port IPv6 Source Guard
Configure the static bound entries of the port IPv6 Source Guard	Configure the static bound entries of the port IPv6 Source Guard
Configure the port MAC static entry binding function	Configure the port MAC static entry binding function
Configure the global IPv6 Source Guard function	Configure the global IPv6 Source Guard function

9.5.2.1 Enable Port IPv6 Source Guard Function

Configuration Condition

None

Enable Port IPv6 Source Guard Function

After enabling the port IPv6 Source Guard function, write the bound entries on the port (including static entries and dynamic entries) to the chip and the packets that completely match the bound entry features can be forwarded. Otherwise, drop it. After enabling IPv6 Source Guard, permit the DHCPv6 packets and ND packets in the port to pass by default.

Table 1065 Enable the port IPv6 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	interface link-aggregation *link-aggregation-id*	
Enable the port IPv6 Source Guard function	ipv6 verify source	Mandatory By default, the port IPv6 Source Guard function is disabled.

9.5.2.2 Configure Max. Bound Entries of Port IPv6 Source Guard

Configuration Condition

Before configuring the maximum number of the port IPv6 Source Guard bound entries, first complete the following task:

- Enable the port IPv6 Source Guard function

Configure Max. Number of Port IPv6 Source Guard Bound Entries

The maximum number of the bound entries (including static, dynamic bound entries) supported by the port prevents one port from being attacked and occupying the device resources.

Table 1066 Configure the maximum number of the port IPv6 Source Guard bound entries

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	interface link-aggregation *link-aggregation-id*	
Configure the maximum number of the port IPv6 Source Guard bound entries	ipv6 verify source max-entries *number*	Mandatory By default, each port can be configured with 536 bound entries.

9.5.2.3 Configure Filtered Packet Type of Port IPv6 Source Guard

Configuration Condition

Before configuring the filtered packet type of the port IPv6 Source Guard, first complete the following task:

- Enable the port IPv6 Source Guard function

Configure Filtered Packet Type of Port IPv6 Source Guard

After enabling the port IPv6 Source Guard function, filter the IPv6 packets by the ip mode. When the source IPv6 address and VLAN number in the IPv6 packet received by the port are the same as the source IPv6 address and VLAN number in the port IPv6 Source Guard bound entries, the port forwards the packet. If any one is different, drop it.

After enabling the port IPv6 Source Guard function, filter the IPv6 packet by the ip-mac mode. When the source MAC address, source IPv6 address and VLAN number in the IPv6 packet received by the port are the same as the MAC address, IPv6 address and VLAN number in the port IPv6 Source Guard bound entry, the port forwards the packet. If any one is different, drop it.

After enabling the port IPv6 Source Guard function, filter the IPv6 packet by the mac mode. When the source MAC address and VLAN number in the IPv6 packet received by the port are the same as the MAC address and VLAN number in the port IPv6 Source Guard bound entry, the port forwards the packet. If any one is different, drop it.

Table 1067 Configure the filtered packet type of the port IPv6 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,
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		the subsequent configuration just takes effect on the aggregation group.
Configure the filtered packet type of the port IPv6 Source Guard	ipv6 verify source type {ip | ip-mac | mac}	Mandatory By default, the port filters the packets by the ip mode.

Note

- After enabling the port IPv6 Source Guard function, the bound entries of the port IPv6 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 IPv6 Source Guard function on the other port, we need to delete the related bound entries of some chip entry resources.
- If some port IPv6 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.
- Configure port IPv6 source guard filter packet type only valid for dynamic entry generated by DHCPv6 snooping

9.5.2.4 Configure Static Bound Entries of Port IPv6 Source Guard

Configuration Condition

Before configuring the static bound entries of the port IPv6 Source Guard, first complete the following task:

- Enable the port IPv6 Source Guard function

Configure Static Bound Entries of Port IPv6 Source Guard

The static bound entries of the port IPv6 Source Guard are the basis of filtering the IPv6 packets received by the specified port.

Table 1068 Configure the static bound entries of the port IPv6 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	interface link-aggregation *link-aggregation-id*	
Configure the static bound entries of the port IPv6 Source Guard	ipv6 source binding { ipv6-address *ipv6-address* [mac-address *mac-address* [vlan *vlan-id*] | vlan *vlan-id*] | mac-address *mac-address* [vlan *vlan-id*] }	Mandatory By default, there is no static bound entry of the port IPv6 Source Guard.

9.5.2.5 Configure Static Entry Binding Function of Port MAC

Configuration Condition

None

Configure Static Entry Binding Function of Port MAC

After configuring the port MAC static entry binding function, get the corresponding mac address, vlan number, and port number from the configured IP Source Guard static entries and got dynamic entries on the port, and deliver the corresponding static MAC entry.

Table 1069 Configure the MAC static entry binding 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	interface link-aggregation *link-aggregation-id*	
Enable the port IP Source Guard function	Ipv6 source sticky-mac	Mandatory By default, the static entry binding function of the port MAC is disabled.

9.5.2.6 Configure Global IPv6 Source Guard Function

Configuration Condition

None

Configure Global IPv6 Source Guard Function

To protect the security of the user IPv6 address and prevent other user from using its own IPv6 address, we can configure the global IPv6 Source Guard function to bind the user IPv6 address and MAC address. The global IP Source Guard bound entries of

the configured user IPv6 address and MAC address are directly written to the chip, so as to filter the invalid IPv6 packets.

Table 1070 Configure the global IPv6 Source Guard function

Step	Command	Description
Enter global configuration mode	config terminal	-
Configure the global IPv6 Source Guard function	ipv6 source binding mac-address *mac-address* ipv6-address *ipv6_address*	Mandatory By default, there is no global IPv6 Source Guard bound entry and the function is disabled.

Note

- The global IPv6 Source Guard bound entries support 40 at most. After exceeding 40, the configuration fails.
- The configured global IPv6 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 IPv6 Source Guard bound entries, we need to delete the related bound entries of some chip entry resources.
- If the port IPv6 Source Guard and global IPv6 Source Guard functions are enabled at the same time, the IP packet received by the port needs to match the bound entries of the port IPv6 Source Guard and global IPv6 Source Guard at the same time so that it can be forwarded. Otherwise, it is dropped.

9.5.2.7 IPv6 Source Guard Monitoring and Maintaining

Table 1071 IPv6 Source Guard monitoring and maintaining

Command	Description
show ipv6 binding table [dynamic | static | interface *interface-name* | slot | summary]	Display the statistics information of the IPv6 Source Guard bound entries and the bound entry quantity
show ipv6 source guard [interface *interface-name*]	Display the configuration information of the port IPv6 Source Guard function

9.5.3 Typical Configuration Example of IPv6 Source Guard

9.5.3.1 Configure Port IPv6 Source Guard Function Based on DHCPv6 Snooping Dynamic Entries

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the global DHCPv6 Snooping function.
- Configure the port IPv6 Source Guard function of the port, so that PC1 can access IP Network normally and PC2 cannot access IP Network.

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet 0/1 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:

On Device, enable global DHCPv6 Snooping function and configure

gigabitethernet0/2 connected to the DHCP Server as the trust port.

```
Device(config)#ipv6 dhcp snooping enable
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#ipv6 dhcp snooping trust
Device(config-if-gigabitethernet0/2)#exit
```

Step 3: Configure the address pool of DHCPv6 Server as 2000::2/64. (omitted)

Step 4: On Device, configure the IPv6 Source Guard function of the port.

#On port gigabitethernet0/1, enable port-based IPv6 Source Guard function.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ipv6 verify source
Device(config-if-gigabitethernet0/1)#exit
```

Step 5: Check the result.

#View the configuration information of DHCPv6 Snooping.

```
Device#show ipv6 dhcp snooping
    dhcpv6-snooping configuration information:
    dhcpv6-snooping status:enable
    dhcpv6-snooping entry aged time:300
    dhcpv6-snooping binding agent save delay time:1800
    dhcpv6-snooping binding agent save type :FLASH
    dhcpv6-snooping binding agent save file :dhcpv6sp_binding.db
    dhcpv6-snooping binding agent save pool time:30
    dhcpv6-snooping interface information :
    ------------------------------------------------------------
    interface          trust-status    max-learning-num option-policy    option18-status
option37-status
    gi0/1          untrust      1024        keep        disable      disable
    gi0/2          trust        1024        keep        disable      disable
    gi0/3          untrust      1024        keep        disable      disable
    gi0/4          untrust      1024        keep        disable      disable
    gi0/5          untrust      1024        keep        disable      disable
    ……
```

#View the configuration information of IPv6 Source Guard.

```
Device#show ipv6 source guard
----------------------------------------
IPv6 source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
------------------------------------------------------
```

```
Interface Name        Status      Verify Type  L2 Status    Max Entry
-------------------------------------------------------
gi0/1              Enabled        ip        Disabled    536
gi0/2              Disabled       ip        Disabled    536
gi0/3              Disabled       ip        Disabled    536
gi0/4              Disabled       ip        Disabled    536
gi0/5              Disabled       ip        Disabled    536
```

We can see that the IPv6 Source Guard function is enabled on port gigabitethernet0/1. Verify Type is ip. Therefore, in the above example, the dynamic entries take effect based on IP+VLAN.

#View the port IPv6 Source Guard bound entry.

```
Device#show ipv6 binding table
-----------------------------global Ipv6 and mac binding entry ------------------------
---
 total :0
-------------------------------------------------------------------------------------
----
-----------------------------------------
IPv6 Source Guard binding table on slot 0
    Total binding entries    : 1
    Static binding entries   : 0
    Static not write entries : 0
    Dynamic binding entries  : 1
    Dynamic not write entries : 0
    PCE writing entries      : 1
-------------------------------------------------------------------------------------
----
Interface-Name  MAC-Address   VLAN-ID  Type-Flag  Writing-Flag   L2-Flag   IP-Address
-------------------------------------------------------------------------------------
----
gi0/1        0001.0001.0001   2       dynamic     Write       Not Write   2000::2
```

#PC1 can access IP Network normally and PC2 cannot access IP Network.

9.5.3.2 Configure Effective Port IPv6 Source Guard Function Based on Static Entries

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.
- Configure the port IPv6 Source Guard function based on static entries, so that PC1 can access IP Network normally and PC2 cannot access IP

Network.

Network Topology

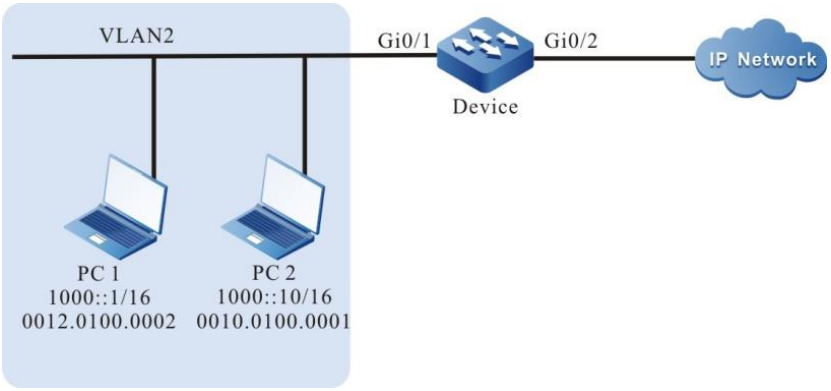


Figure 225 Networking of configuring effective port IPv6 Source Guard function based on static entries

Configuration Steps

Step 1: Configure the link type of 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, 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 IPv6 Source Guard function on Device.

#Enable the port IPv6 Source Guard function based on MAC+VLAN filtering mode on port gigabitethernet0/1, and configure the IP address as 1000::1, and the port IPv6 Source Guard bound entry of VLAN 2.

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ipv6 verify source
Device(config-if-gigabitethernet0/1)#ipv6 source binding ip-address 1000::1 vlan 2
```

```
Device(config-if-gigabitethernet0/1)#exit
```

Step 3: Check the result.

View the configuration information of IPv6 Source Guard.

```
Device#show ipv6 source guard
----------------------------------------
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
------------------------------------------------------------
Interface Name        Status     Verify Type  L2 Status
------------------------------------------------------------
gi0/1              Enabled        IP       Disabled
gi0/2              Disabled       IP       Disabled
gi0/3              Disabled       IP       Disabled
gi0/4              Disabled       IP       Disabled
```

We can see that the IPv6 Source Guard function is enabled on port gigabitethernet0/1. The static IPv6 Source Guard entry takes effect according to the configured MAC+VLAN entry, not related with the Verify Type value. Therefore, the above example takes effect based on MAC+VLAN.

#View the port IPv6 Source Guard bound entry.

```
Device #show ipv6 binding table
----------------------------global Ipv6 and mac binding entry ----------------------------
---
 total :0
------------------------------------------------------------------------------------------
----
----------------------------------------
IPv6 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  VLAN-ID  Type-Flag  Writing-Flag  L2-Flag  IP-Address
------------------------------------------------------------------------------------------
----
gi0/1          ---          2       Static     Write         Not Write  1000::1
```

#PC1 can access IPv6 Network normally and PC2 cannot access IP Network.

9.6 ND Snooping

9.6.1 Overview

ND Snooping

ND snooping is a security feature of IPv6 ND (neighbor discovery), which is used in L2 switching network environment. The dynamic binding table of ND snooping is established by listening to neighbor request packet NS (neighbor solicitation) in the process of detecting DAD (duplicate address detection) of users, so as to record the source IPv6 address, source MAC address, VLAN, ingress port and other information of the packet, so as to prevent the subsequent ND packet attack of counterfeited users and gateway.

ND Snooping trust interface/non-trust interface

ND Snooping trust interface: This type of interface is used to connect trustable IPv6 nodes. For the ND packets received from this type of interface, the device forwards normally.

ND Snooping non-trust interface: This type of interface is used to connect un-trustable IPv6 nodes. For RA packets and redirection packets received from this type of interface, the device considers them as illegal packets and drop them directly. For NA/NS/RS packets received, if the VLAN where this interface or interface is located enables the ND packet validity check function, the device will use ND Snooping dynamic binding table to perform the matching check of the binding table for NA/NS/RS packets. When the packet does not conform to the binding table relationship, the packet is regarded as the illegal user packet and dropped directly; for other types of ND packet received, the device forwards normally.

ND Snooping binding table

After the ND snooping function is configured, the device establishes the ND Snooping dynamic binding table by listening to the NS packet used by the user for

repeated address detection. The entries include the request IPv6 address, source MAC address, VLAN, ingress interface and other information in the DAD packet. ND snooping dynamic binding table can be used to perform the matching check of the binding table for NA/NS/RS packets received from untrusted interfaces, so as to filter illegal NA/NS/RS packets.

9.6.2 ND Snooping Function Configuration

Table 1072 ND Snooping function configuration list

Configuration Task	
Enable the ND Snooping function	Enable the ND Snooping function
Specify the ND Snooping trust interface	Specify the ND Snooping trust interface
Configure ND Snooping static binding entry	Configure ND Snooping static binding entry
Configure the detection function of ND Snooping dynamic binding table	Configure the detection function of ND Snooping dynamic binding table
Enable ND Snooping attack detection log function	Enable ND Snooping attack detection log function

9.6.2.1 Enable ND Snooping Function

Configuration Condition

None

Enable ND Snooping Function

Table 1073 Enable the ND Snooping function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable global ND Snooping function	nd snooping enable	Mandatory By default, the global ND Snooping function is disabled.
Enter the L2 VLAN configuration mode	vlan *vlan-id*	Mandatory After entering the L2 VLAN configuration mode, the

Step	Command	Description
		subsequent configuration takes effect only in the current VLAN.
Enable the ND Snooping function in the VLAN	nd snooping enable	Mandatory By default, the ND Snooping function is not enabled in VLAN.

9.6.2.2 Specify ND Snooping Trust Interface

Configuration Condition

None

Specify ND Snooping Trust Interface

Table 1074 Specify the ND Snooping trust interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable global ND Snooping function	nd snooping enable	Mandatory By default, the global ND Snooping function is disabled.
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	Mandatory After entering the L2 Ethernet interface configuration mode, the subsequent configuration takes effect only for the current port.
Specify the ND Snooping trust interface	nd snooping trusted	Mandatory By default, the interface is the non-trust interface.

9.6.2.3 Configure ND Snooping Static Binding Entry

Configuration Condition

None

Configure ND Snooping Static Binding Entry

Table 1075 Configure ND Snooping static binding entry

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable global ND Snooping function	nd snooping enable	Mandatory By default, the global ND Snooping function is disabled.
Configure ND Snooping static binding entry	nd snooping user-bind *ipv6-address mac-address* vlan *vlan-id* interface *interface-name*	Optional By default, do not configure the ND snooping static binding entry. When the static binding entry is configured, first match the static binding entry. When the static binding entry is not configured, directly use the dynamic binding entry.

9.6.2.4 Configure the Detection Function of ND Snooping Dynamic Binding Table

Configuration Condition

None

Configure the Detection Function of ND Snooping Dynamic Binding Table

Table 1076 Configure the detection function of ND Snooping dynamic binding table

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable global ND Snooping function	nd snooping enable	Mandatory By default, the global ND Snooping function is disabled.
Configure the detection function of ND Snooping dynamic binding table	nd snooping detect retransmit *retransmits-times* interval *time*	Mandatory By default, the detection function of ND Snooping dynamic binding table is not enabled.

9.6.2.5 Enable ND Snooping Attack Detection Log Function

Configuration Condition

None

Enable ND Snooping Attack Detection Log Function

Table 1077 Enable the ND Snooping attack detection log function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable global ND Snooping function	**nd snooping enable**	Mandatory By default, the global ND Snooping function is disabled.
Enable the ND Snooping attack detection log function	**nd snooping attack-log enable**	Mandatory By default, the ND Snooping attack detection log function is disabled.

9.6.2.6 ND Monitoring and Maintaining

Table 1078 ND Monitoring and Maintaining

Command	Description
clear nd fast-response statistics	Clear the ND fast response statistics
clear nd snooping dynamic-user-bind	Delete ND snooping dynamic binding entries
clear nd snooping prefix	Delete ND snooping prefix entry
clear nd snooping statistics	Clear ND snooping statistics information
show nd fast-response statistics	Display the ND fast response statistics
show nd proxy address	Display the address with ND as external module response
show nd snooping prefix	Display the ND snooping prefix entry
show nd snooping user-bind	Display the ND snooping binding entry
show nd snooping statistics	Display the ND snooping statistics information

9.6.3 ND Snooping Typical Configuration Example

9.6.3.1 Configure ND Snooping Basic Function

Network Requirements

- Device 1 is connected to gateway Device 2 through gigabitothernet0/3.
- Device 2 enables RA service (enables RA packet sending function).
- Device 1 enables ND snooping function. When an attacker sends illegal NS/NA/ RS /RA packets in the network, Device1 discards these invalid ND packets to ensure the communication between the valid user and the gateway.

Network Topology

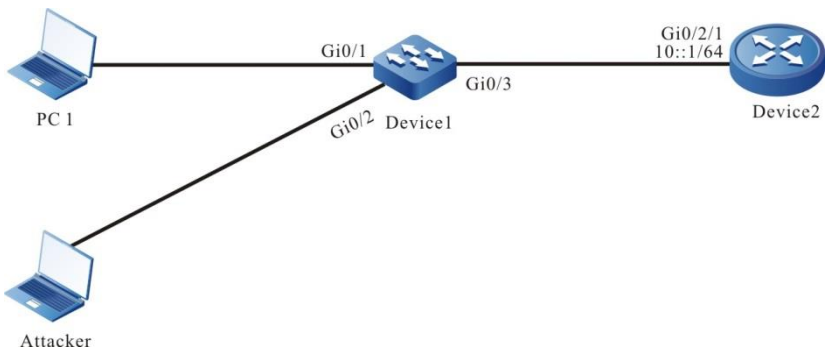


Figure 226 Networking of configuring ND Snooping basic functions

Configuration Steps

Step 1: On Device1, configure the VLAN and port link type.

#Create VLAN2.

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#Configure the link type of port gigabitethernet0/1-gigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/1-0/3
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

Step 2: On L3 interface gigabitethernet0/2/1 of gateway device Device2, configure the IPv6 address.

```
Device2(config)#interface gigabitethernet 0/2/1
Device2 (config-if-gigabitethernet0/2/1)#ipv6 address 10::1/64
Device2 (config-if-gigabitethernet0/2/1)#exit
```

Step 3: On the gateway device Device2, enable the RA service (enable the RA packet sending function).

```
Device2(config)#interface gigabitethernet 0/2/1
Device2 (config-if-gigabitethernet0/2/1)#no ipv6 nd suppress-ra period
Device2 (config-if-gigabitethernet0/2/1)#no ipv6 nd suppress-ra response
Device2 (config-if-gigabitethernet0/2/1)#exit
```

Step 4: On Device1, configure the ND Snooping function.

#Globally enable the ND Snooping function.

```
Device1(config)#nd snooping enable
```

#VLAN2 enables the ND Snooping function.

```
Device1(config)#vlan 2
Device1(config-vlan2)#nd snooping enable
Device1(config-vlan2)#exit
```

#Configure port gigabitethernet0/3 as trust interface.

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#nd snooping trusted
Device1(config-if-gigabitethernet0/3)#exit
```

Step 5: Check the result.

#View that Device1 gets the prefix information sent by the gateway device Device2.

```
Device1#show nd snooping prefix
   prefix                    length    valid-time       preferred-time
   ------------------------------------------------------------------------------
---
   10::                      64        2592000          604800

   Total number: 1
```

#After PC1 configure the IPv6 address 10::3 in the management range of the prefix 10::/64, view the ND Snooping entry on Device.

```
Device1#show nd snooping user-bind dynamic
ipv6-address      mac-address       vlan     interface        type
10::3             0857.00da.4715    2        gi0/1            dynamic
```

On Device1, generate the ND Snooping entry of the IP, MAC, VLAN, access port information of PC1.

#Attacker simulates the IP of PC1 to send NS, NA, and RS packets to the gateway. The device receives the NS, NA, RS packets from the attacker, judges that it is inconsistent with the recorded ND snooping entry, discards it, and makes relevant records in the ND snooping statistics information.

```
Device1#show nd snooping statistics

   Statistics for lpu 0 nd snooping:

   lladdrInvalid:          0
   dadPacketDeal:          0
   nsPacketPass:           0
   nsPacketDrop:           1
   naPacketPass:           0
   naPacketDrop:           1
```

```
rsPacketDrop:          1
rsPacketPass:          0
raPacketPass:          0
raPacketDrop:          0
rdPacketDrop:          0
rdPacketPass:          0
sendDtPktFail:         0
sendDtPktOk:           0
```

#Attacker simulates the gateway to send the RA packet to PC1. Device receives the RA packet of Attacker, judges that the RA packet is received from the un-trust packet, drops it, and makes the related records in the ND Snooping statistics information.

```
Device1#show nd snooping statistics

Statistics for lpu 0 nd snooping:

lladdrInvalid:         0
dadPacketDeal:         0
nsPacketPass:          0
nsPacketDrop:          0
naPacketPass:          0
naPacketDrop:          0
rsPacketDrop:          0
rsPacketPass:          0
raPacketPass:          0
raPacketDrop:          1
rdPacketDrop:          0
rdPacketPass:          0
sendDtPktFail:         0
sendDtPktOk:           0
```

9.7 DHCP Snooping

9.7.1 Overview

9.7.1.1 Overview of DHCP Snooping Basic Functions

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.

1. 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.

9.7.1.2 Brief Introduction of DHCP Snooping Option82

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.

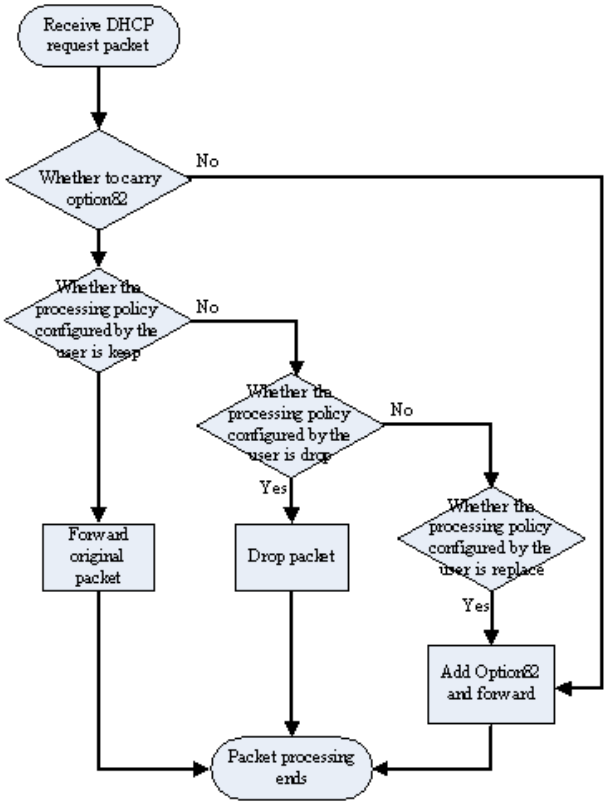


Figure 227 Processing flow of Option82

1. 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.

9.7.2 DHCP Snooping Function Configuration

Table 1079 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

Configuration Task	
	function
Configure DHCP Snooping Option82	Configure the processing policy of Option82
	Configure the Remote ID content
	Configure the Circuit ID content
	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

9.7.2.1 Configure DHCP Snooping Basic Functions

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 Condition

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 1080 Configure the DHCP Snooping function

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
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 1081 Configure the 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	interface 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 1082 Configure the 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	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
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.

9.7.2.2 Configure DHCP Snooping Option82

The DHCP Snooping function supports Option82. Option82 can contain 255 sub options at most. Sofinet device supports two sub options, that is, Circuit ID and Remote ID.

Configuration Condition

Before configuring DHCP Snooping Option82, first complete the following task:

- Enable the DHCP Snooping function

Configure the Processing Policy of Option82

After the port is configured with the disable information, whatever option packet

the port receives, it is forwarded as it is.

Table 5 Configure the processing policy of Option82

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the Option82 of the DHCP Snooping function	dhcp-snooping information enable	Mandatory By default, the Option82 of the DHCP Snooping function is disabled.
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	interface link-aggregation *link-aggregation-id*	
Configure the processing policy of Option82	dhcp-snooping information disable	Optional By default, the processing policy for the DHCP request packet with Option82 is replace, that is, forward after replacing.

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:

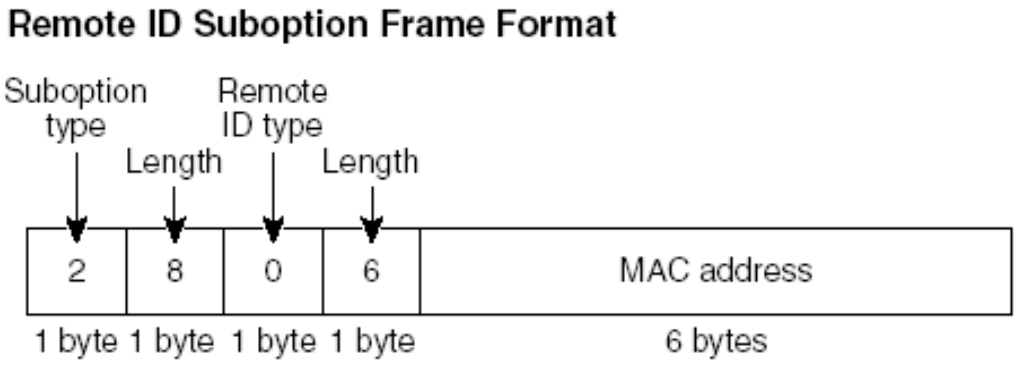


Figure 228 The filling format of the default content of Remote ID

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:

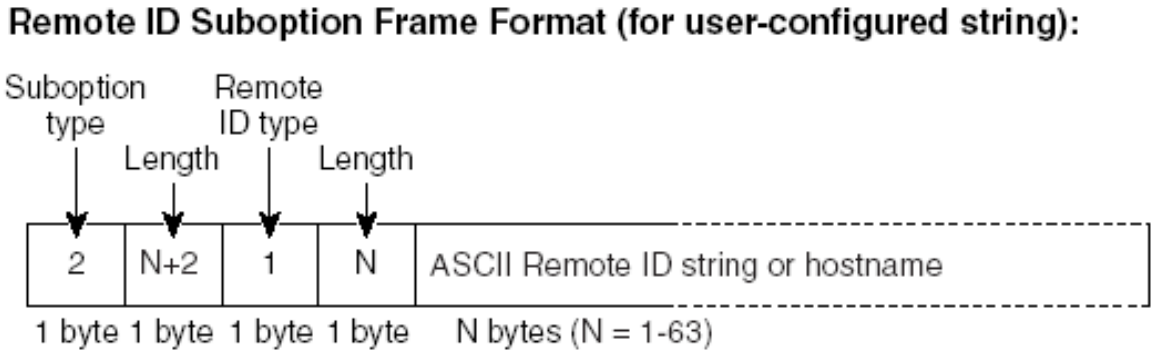


Figure 229 The filling format of the non-default content of Remote ID

Table 1083 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:

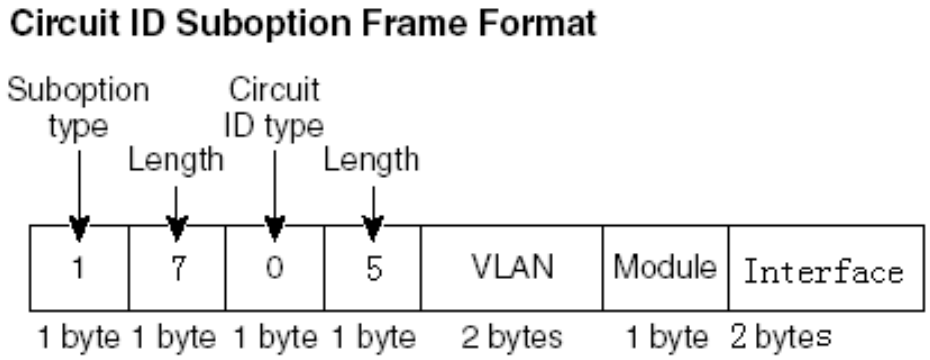


Figure 230 The filling format of the default content of Circuit ID

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:

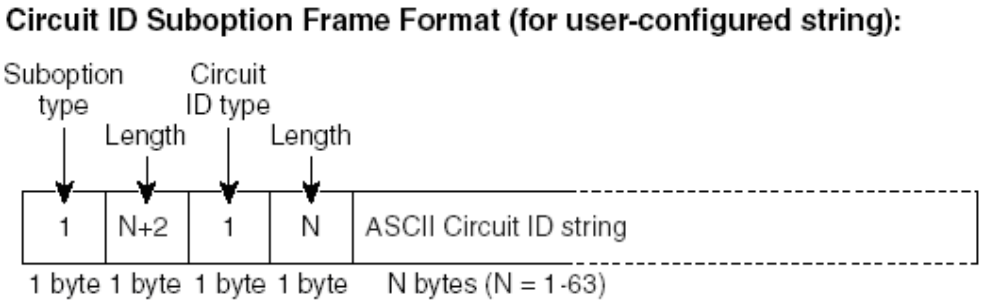


Figure 231 The filling format of the non-default content of Circuit ID

Table 1084 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		subsequent configuration just takes effect on the aggregation group.
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 1085 Configure the 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 1086 Configure the packet processing policy of Option82

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure the packet processing policy of Option82	dhcp-snooping information policy { drop | keep | replace }	Mandatory By default, the processing policy is replace.

9.7.2.3 Configure Storing of DHCP Snooping Bound Entries

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 Condition

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 1087 Configure the 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	dhcp-snooping database savetype auto { flash *file-name*	Mandatory By default, the storing mode of

Step	Command	Description
entries	| ftp *dest-ip-address ftp-username ftp-password file-name* | tftp *dest-ip-address file-name* }	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 1088 Configure the manual storing of the 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

Step	Command	Description
		path.

9.7.2.4 Monitoring and Maintaining of DHCP Snooping

Table 1089 DHCP Snooping monitoring and maintaining

Command	Description
clear dhcp-snooping database { interface { *interface-list* | link-aggregation *link-aggregation-id* } | ip-address *ip-address* | mac-address *mac-address* | vlan *vlan-id* | all }	Clear the bound entries
clear dhcp-snooping packet statistics [interface { *interface-name* | link-aggregation *link-aggregation-id* }]	Clear the statistics information of the sent and received DHCP packets
show dhcp-snooping [interface { *interface-name* | link-aggregation *link-aggregation-id* } | save | detail]	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* } | ip-address *ip-address* | vlan *vlan-id*| mac-address *mac-address* [| { { begin | exclude | include } *expression* | redirect { file *file-name* | ftp [vrf *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }] | detail]	Display the DHCP Snooping bound entry information
show dhcp-snooping packet statistics [interface { *interface-name* | link-aggregation *link-aggregation-id* }]	Display the statistics information of the sent and received DHCP packets

9.7.3 Typical Configuration Example of DHCP Snooping

9.7.3.1 Configure DHCP Snooping Basic Functions

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

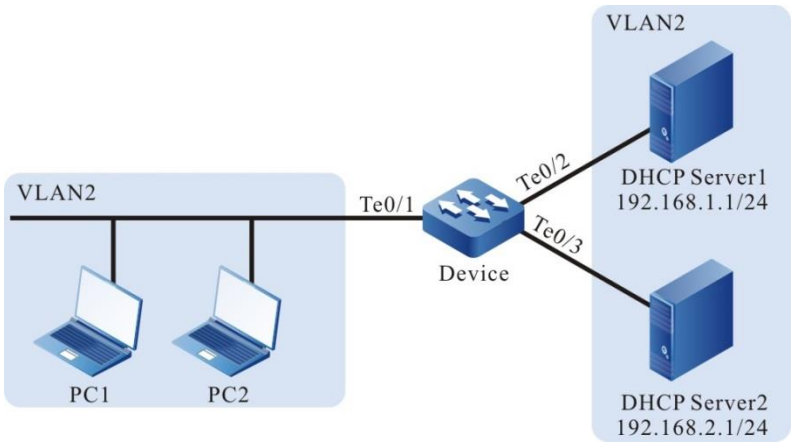


Figure 232 Networking of configuring DHCP Snooping basic functions

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port tengigabitethernet0/1-tengigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 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 tengigabitethernet0/2 as trust port.

```
Device(config)#interface tengigabitethernet 0/2
Device(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device(config-if-tengigabitethernet0/2)#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     te0/1          107990         active
    ------
    0013.0100.0001 192.168.1.100  0           2     te0/1          107989         active
    ------
Total valid DHCP Client binding table for this criterion: 2
```

PC1 and PC2 both can get address from DHCP Server1.

9.8 DHCPv6 Snooping

9.8.1 Overview

9.8.1.1 Introduction to DHCPv6 snooping Basic Functions

DHCPv6 snooping is one security feature of DHCPv6 (Dynamic Host Configuration Protocol for IPv6) and has the following two functions:

Record the corresponding relation of the MAC address and IPv6 address of the DHCPv6 client:

Considering the security, the network administrator may need to record the IPv6 address used when the user accesses the network, confirming the corresponding

relation of the user host IPv6 address and the IPv6 address got from the DHCPv6 server.

DHCPv6 snooping listens to the DHCPv6 request packet and the DHCPv6 response packet received by the trust port and records the MAC address of the DHCPv6 client and the obtained IPv6 address. The administrator can view the IPv6 address information got by the DHCPv6 client via the bound entry recorded by DHCPv6 snooping.

1. Ensure that the client gets the IPv6 address from the valid server

If there is unauthorized DHCPv6 server in the network, the DHCPv6 client may get the wrong IPv6 address, resulting in the communication abnormality or security risks. To ensure that the DHCPv6 client can get the IPv6 address from the valid DHCPv6 server, the DHCPv6 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 DHCPv6 server. The trust port forwards the received DHCPv6 response packet normally, so as to ensure that the DHCPv6 client can get the correct IP address.
- Un-trust port is the port not directly or indirectly connected to the valid DHCPv6 server. If the un-trust port receives the DHCPv6 response packet sent by the DHCPv6 server, drop it, so as to prevent the DHCPv6 client from getting the wrong IPv6 address.

9.8.1.2 Brief Introduction of DHCPv6 snooping Option18/37

To make DHCPv6 Server get the physical location information of the DHCPv6 client, you can add Option18 and Option37 to the DHCPv6 request packet.

When the device detects the DHCPv6 packet, it can add some user device information to the DHCPv6 request packet by the DHCPv6 Option mode. Option18 records the interface information of the client, and is called interface ID option

(interface ID). Option37 records the MAC address information of the client and is called remote ID option (Remote ID).

When Option18/37 is enabled and after the device receives the DHCPv6 request packet, provide the following processing according to the processing policy and filling mode of the Option18/37 configured by the user.

Table 1090 The processing policy of the DHCPv6 request packet

DHCPv6 request packet	Processing policy	Filling Mode	Packet Processing Principle
Without Option18/37	Add	Default Filling format	Fill in and forward according to the default format
	Add	Extended filling format	Fill in and forward according to the customized format of the user
With Option18/37	Keep	Do not fill	Forward without processing Option18/37
	Replace	Default filling format	Replace the original Option18/37 content and forward according to the default format
		Extended filling format	Replace the original Option18/37 content and forward according to the customized format of the user

9.8.2 DHCPv6 snooping Function Configuration

Table 1091 DHCPv6 snooping function configuration list

Configuration Task	
Configure DHCPv6 snooping basic functions	Enable DHCPv6 snooping
	Configure the port trust status
	Configure the number of the port bound entries
Configure DHCPv6 snooping Option18/37	Configure Option18
	Configure Option37
	Configure the processing policy of the Option18/37 packet
Configure the delay time of deleting the DHCPv6	Configure the delay time of deleting the

Configuration Task	
snooping invalid entry	DHCPv6 snooping invalid entry
Configure the storing of the DHCPv6 snooping bound entries	Configure the storing of the DHCPv6 snooping bound entries

9.8.2.1 Configure DHCPv6 snooping Basic Functions

DHCPv6 snooping basic functions include enable the DHCPv6 snooping function, configure the port trust status, and configure the number of the port DHCPv6 snooping bound entries.

Configuration Condition

None

Enable DHCPv6 snooping

After enabling the DHCPv6 snooping function, monitor the DHCPv6 packets received by all ports of the device.

- For the received DHCPv6 request packet, generate the corresponding bound entry according to the information in the packet
- For the response packet received by the trust port, update the status and lease time of the corresponding bound entries
- For the response packet received by the un-trust port, drop it directly

Table 1092 Enable DHCPv6 snooping

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable the DHCPv6 snooping function	ipv6 dhcp snooping enable	Either By default, the DHCPv6 snooping function is disabled.
Enable the DHCPv6 snooping function of the specified VLAN	ipv6 dhcp snooping vlan *vlanlist*	

Configure Port Trust Status

To prevent the DHCPv6 client from getting the address from the invalid DHCPv6 server, you can configure the port directly or indirectly connected to the valid server as the trust port.

After the port is configured as the trust port, permit the DHCPv6 response packet to be forwarded normally. Otherwise, drop the DHCPv6 response packet.

Table 1093 Configure the 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	interface link-aggregation *link-aggregation-id*	
Configure the port trust status	ipv6 dhcp snooping trust	Mandatory By default, all ports are un-trust port.

Note

- The port connected to the DHCPv6 server needs to be configured as the trust port. Otherwise, the DHCPv6 client cannot get the address.

Configure the Number of Port DHCPv6 snooping Bound Entries

Configuring the number of the DHCPv6 snooping bound entries can limit the maximum number of the dynamic entries that can be learned by the port, preventing occupying too many system resources.

Table 1094 Configure the number of the port DHCPv6 snooping bound entries

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	interface link-aggregation *link-aggregation-id*	
Configure the number of the DHCPv6 snooping bound entries	ipv6 dhcp snooping max-learning-num *number*	Mandatory By default, the number of the bound entries that can be learned by the port is 1024.

9.8.2.2 Configure DHCPv6 snooping Option18/37

The DHCPv6 snooping function supports Option18 and Option37. Option18 and Option37 both support the default filling format and extended filling format.

Configuration Condition

Before configuring the DHCP snooping Option18 and Option37, first complete the following task:

- Enable the DHCPv6 snooping function

Configure Option18

The content of Interface ID includes default filling format and extended filling format. The default content filling format of Interface ID is as follows:

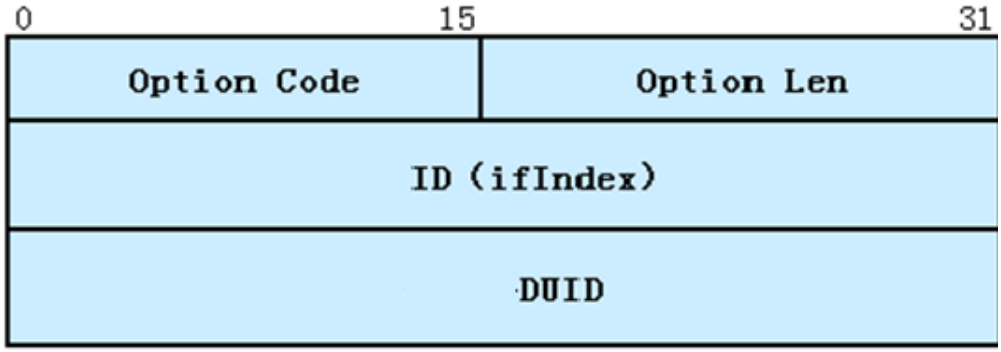


Figure 233 The default content filling format of Interface ID

The extended filling format needs the filling format to be configured to take effect in the user configuration format. The extended filling format of Interface ID is as follows:

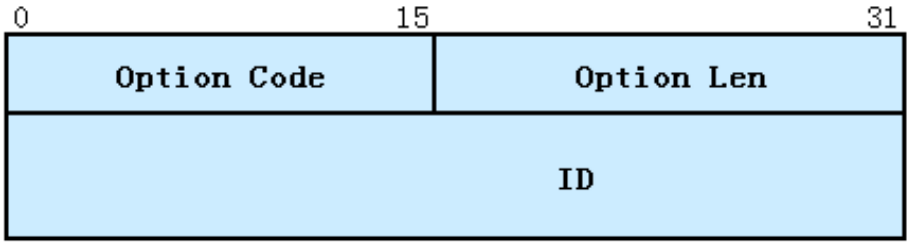


Figure 234 The extended filling format of Interface ID

Table 1095 Configure Option18

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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enable Option18 function	ipv6 dhcp snooping option interface-id enable	Mandatory By default, Option18 is disabled.
Configure the content of Interface ID	ipv6 dhcp snooping option format interface-id *LINE*	Optional By default, the Interface ID content in Option18 is interface id – duid format.

Configure Option37

The content of Remote ID includes default filling format and extended filling format. The default content filling format of Remote ID is as follows:

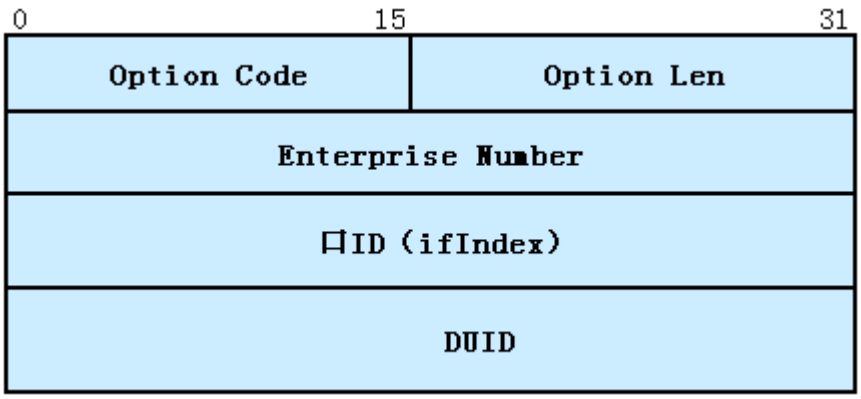


Figure 235 The default content filling format of Remote ID

The extended filling format needs the filling format to be configured to take effect in the user configuration format. The extended filling format of Remote ID is as follows:

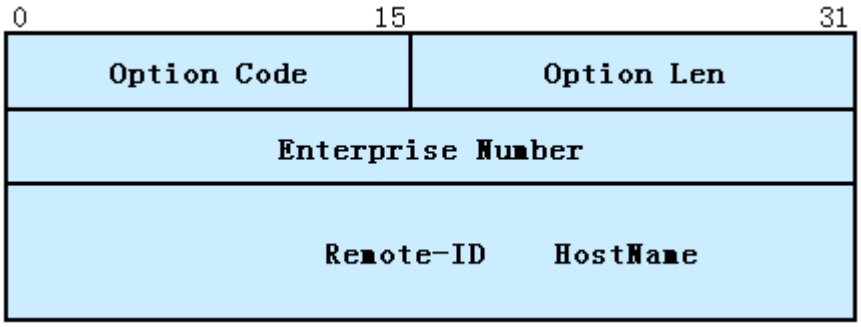


Figure 236 The non-default content filling format of Remote ID

Table 1096 Configure Option37

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	interface link-aggregation *link-aggregation-id*	
Enable Option37 function	ipv6 dhcp snooping option remote-id enable	Mandatory By default, the Option37 function is disabled.
Configure the content of Remote ID	ipv6 dhcp snooping option format remote-id { *LINE* | hostname }	Mandatory By default, the Remote ID content in Option37 is enterprise num - interface id –duid format.

Configure the Processing Policy of Option18/37 Packet

After configuring the processing policy of the Option18/37 packet, you can adopt different processing policies for the DHCPv6 request packet with Option18/37.

Table 1097 Configure the processing policy of the Option18/37 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	interface link-aggregation *link-aggregation-id*	
Configure the processing policy of the Option18/37 packet	ipv6 dhcp snooping option policy replace	Mandatory By default, do not replace the Option18/37 content in the DHCPv6 request packet.

9.8.2.3 Configure Delay Time of Deleting DHCPv6 snooping Invalid Entry

Configuration Condition

Before configuring the delay time of deleting the DHCPv6 snooping invalid entry, first complete the following task:

- Enable the DHCPv6 snooping function

Configure Delay Time of Deleting DHCPv6 snooping Invalid Entry

After deleting the binding relationship, the bound entry is updated to invalid. The invalid entry is not deleted immediately, but is deleted after exceeding the delay time. During the period, if the client renews the lease, the bound entry can be activated, but do not need to re-set up the bound entry.

Table 1098 Configure the delay time of deleting the DHCPv6 snooping invalid entry

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the delay time of deleting the DHCPv6 snooping invalid entry	ipv6 dhcp snooping database timeout *seconds*	Mandatory By default, the delay time of deleting the DHCPv6 snooping invalid entry is 300s.

9.8.2.4 Configure Storing of DHCPv6 snooping Bound Entries

The DHCPv6 snooping function supports the auto or manual storing to the device FLASH. If the device restarts, the stored bound entries can be restored, avoiding affecting the communication because the bound entries are lost.

Configuration Condition

Before configuring the storing of the DHCPv6 snooping bound entries, first complete the following task:

- Enable the DHCPv6 snooping function

Configure the Storing of DHCPv6 snooping Bound Entries

The system periodically refreshes the DHCPv6 snooping 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. Meanwhile, you also can store the bound entries to the device FLASH immediately.

Table 1099 Configure the storing of the DHCPv6 snooping bound entries

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure the refresh interval of the DHCPv6 snooping bound entries	ipv6 dhcp snooping database save pool *seconds*	Optional By default, the refresh interval of the DHCPv6 snooping bound entries is 30s.
Configure the storing delay of the DHCPv6 snooping bound entries	ipv6 dhcp snooping database save interval *seconds*	Optional By default, the storing delay of the DHCPv6 snooping bound entries is 1800s.
Configure storing the bound entries immediately	ipv6 dhcp snooping database save now	Optional By default, the storing delay of the bound entry is 1800s.
Configure storing the DHCPv6 snooping bound entries to the specified file	ipv6 dhcp snooping database save filename *string*	Mandatory By default, the storing file name is /flash/dhcpv6sp_binding.db.

9.8.2.5 DHCPv6 snooping Monitoring and Maintaining

Table 1100 DHCPv6 snooping monitoring and maintaining

Command	Description
clear ipv6 dhcp snooping database [interface { *interface-list* } | ipv6-address *ipv6-address* | *mac-address* | vlan *vlan-id*]	Clear the DHCPv6 Snooping binding entry
clear ipv6 dhcp snooping statistics [interface { *interface-name* }]	Clear the statistics information of the received and sent DHCPv6 packets
show ipv6 dhcp snooping [interface { *interface-name* }]	Display the DHCPv6 Snooping configuration information on the specified interface
show ipv6 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*	Display the DHCPv6 Snooping bound entry information

Command	Description
} | ipv6-address *ipv6-address* | mac-address *mac-address* | vlan *vlan-id*] [| { { begin | exclude | include } *expression* | redirect { file *file-name* | ftp [vrf *vrf-name*] { *hostname* | *dest-ip-address* } *ftp-username ftp-password file-name* } }]]	
show ipv6 dhcp snooping statistics [interface { *interface-name* }]	Display the statistics information of the received and sent DHCPv6 packets

9.8.3 Typical Configuration Example of DHCPv6 snooping

9.8.3.1 Configure DHCPv6 Snooping Basic Functions

Network Requirements

- DHCPv6 Server1 is the valid DHCPv6 server; DHCPv6 Server2 is the invalid DHCPv6 server.
- After configuring the DHCPv6 snooping function, PC1 and PC2 both can get address from DHCPv6 Server1.

Network Topology

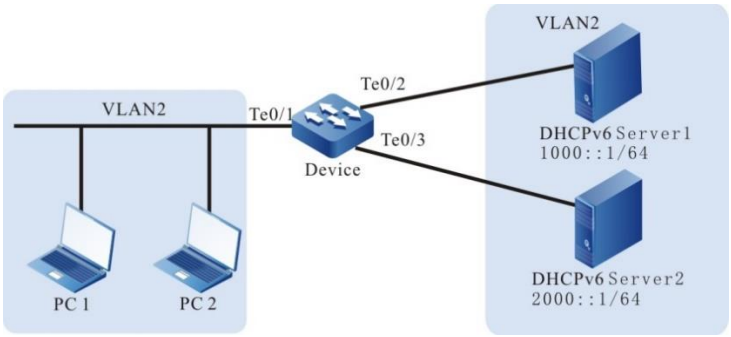


Figure 237 Networking of configuring DHCPv6 snooping basic functions

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device.

#Create VLAN2.

```
Device#configure terminal
```

```
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port tengigabitethernet0/1-tengigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 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 DHCPv6 Server1 as 1000::2/64 and the address pool of DHCPv6 Server2 as 2000::2/64. (Omitted)

Step 3: Configure the DHCPv6 snooping function on Device.

#Enable the DHCPv6 snooping function.

```
Device(config)#ipv6 dhcp snooping enable
```

#Configure the port tengigabitethernet0/2 as trust port.

```
Device(config)#interface tengigabitethernet 0/2
Device(config-if-tengigabitethernet0/2)#ipv6 dhcp snooping trust
Device(config-if-tengigabitethernet0/2)#exit
```

Step 4: Check the result.

#After PC1 and PC2 get the address successfully, view the DHCPv6 snooping entries on Device.

```
Device#show ipv6 dhcp snooping database
 Interface-Name      MAC-Address     VLAN-ID  ValidTime  AgedTime   IP-Address
 te0/1           0001.0001.0008    2       120        0        1000::2
 te0/1           0001.0001.0007    2       120        0        1000::3
```

PC1 and PC2 both can get address from DHCPv6 Server1.

9.9 Dynamic ARP Inspection

9.9.1.1 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:

- 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 binding 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 binding entry, the ARP packet is valid packet and is forwarded. Otherwise, the ARP packet is invalid packet, drop it, and record the log information.

- Global DAI function: Check the validity of the ARP packets received by all ports, so as to prevent fake users from sending forged ARP packets, resulting in incorrect ARP entries.

The ARP message validity detection is based on the global IP source guard binding entry. The specific detection principle is as follows:

When in the received ARP packet, the IP address of the sender is the same as the IP address in the binding entry of the global IP source guard, but the source MAC address is different, judge the ARP packet as a forged packet, and drop it without recording the log information.

The port DAI, global DAI function also checks 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.

9.9.2 Dynamic ARP Inspection Function Configuration

Table 1101 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

9.9.2.1 Configure Port Dynamic ARP Inspection Function

Configuration Condition

Before configuring the port Dynamic ARP Inspection function, first complete the following task:

- Configure the port IP Source Guard binding entry

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 IP Source Guard binding entry. 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 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 20s exceed the rate, disable the port to isolate the packet impact source.

Table 1102 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
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.
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.

Step	Command	Description
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.

9.9.2.2 Configure Global Dynamic ARP Inspection Function

Configuration Condition

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 will perform the validity check for the received ARP packet according to the global IP Source Guard bound entry. If it is the invalid packet, drop it directly, and do not record the log.

Table 1103 Configure the global Dynamic ARP Inspection function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable global DAI function	arp-security	Mandatory By default, the global DAI function is disabled.

9.9.2.3 Configure Dynamic ARP Attack Inspection

Configuration Condition

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 1104 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		subsequent configuration can only take effect in the aggregation group.
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.

9.9.2.4 Monitoring and Maintaining of Dynamic ARP Inspection

Table 1105 Dynamic ARP Inspection monitoring and maintaining

Command	Description
clear ip arp inspection { log-information | log-statistics | pkt-statistics [interface { *interface-name* | link-aggregation *link-aggregation-id* }] }	Delete the statistics information recorded by the DAI function
show arp-security	Display the global DAI function status
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
show ip arp inspection pkt-statistics [interface { *interface-name* | *link-aggregation link-aggregation-id* }]	Display the statistics information of the ARP packets

9.9.3 DAI Typical Configuration Example

9.9.3.1 Configure DAI Basic Function

Network Requirements

- PC1 and PC2 are connected to IP Network via Device.

- On Device, configure the DAI function of the port, preventing the ARP attack and spoofing.

Network Topology

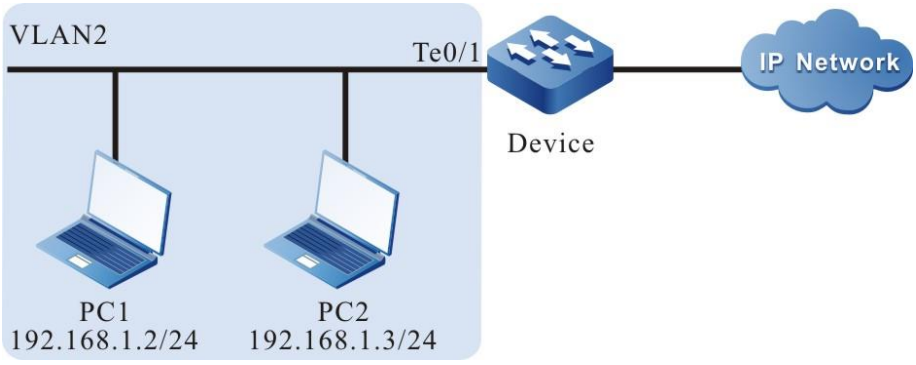


Figure 238 Networking of configuring DAI basic functions

Configuration Steps

Step 1: On Device, configure the VLAN and port link type.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port tengigabitethernet0/1 as Access, permitting the services of VLAN2 to pass.

```
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: Configure the port DAI function on Device.

#Enable port DAI function on port tengigabitethernet0/1, and configure the upper limit of port tengigabitethernet0/1 processing ARP packets as 30pps.

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip arp inspection
Device(config-if-tengigabitethernet0/1)#ip arp inspection rate-limit 30
Device(config-if-tengigabitethernet0/1)#exit
```

Step 3: On Device, configure the binding entry.

#On port tengigabitethernet0/1, configure MAC address as 0012.0100.0001, IP address as 192.168.1.2, and port IP Source Guard binding entry of VLAN2.

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip source binding ip-address 192.168.1.2 mac-address 0012.0100.0001 vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

Step 4: Check the result.

#Query the DAI related 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
    te0/1            enable    30               OFF
    te0/2            disable   15               OFF
```

#When the rate of receiving ARP packets by port tengigabitothernet0/1 exceeds 30pps, Device will discard the packets exceeding the rate and output the following prompt message.

```
Jan  1 02:21:06: The rate on interface tengigabitethernet0/1 too fast ,the arp packet drop!
```

#When the rate of receiving ARP packets by port tengigabitothernet0/1 exceeds 30pps and lasts for 20 seconds, Device will close port tengigabitothernet0/1 and output the following prompt information.

```
Jan  1 02:21:26: %LINK-INTERFACE_DOWN-4: interface tengigabitethernet0/1, changed state to down
Jan  1 02:21:26: The rate of arp packet is too fast,dynamic arp inspection shut down the tengigabitethernet0/1 !
```

#When the ARP packets received by port tengigabitothernet0/1 is inconsistent with the binding entry, Device records the illegal information in the following format to the DAI log and outputs it 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: tengigabitethernet0/1 record packet :32 packet(s)

#View the DAI log.

```
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: tengigabitethernet0/1 record packet :0 packet(s)
```

9.9.3.2 DAI Combining With DHCP Snooping

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

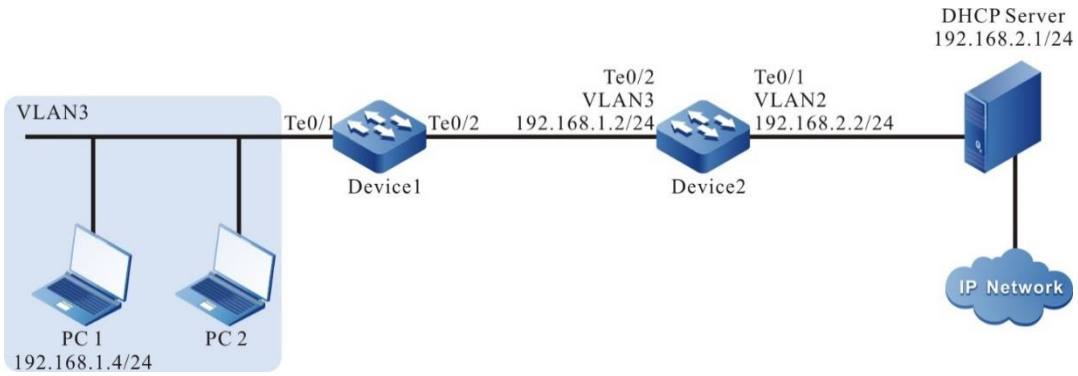


Figure 239 Networking of combing DAI with DHCP Snooping

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 tengigabitethernet0/1 and tengigabitethernet0/2

as Access, permitting the services of VLAN3 to pass.

```
Device1(config)#interface tengigabitethernet 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 tengigabitethernet0/1 and tengigabitethernet0/2 as Access; port tengigabitethernet0/1 permits the services of VLAN2 to pass; port tengigabitethernet0/2 permits the services of VLAN3 to pass.

```
Device2(config)#interface tengigabitethernet 0/1
Device2(config-if-tengigabitethernet0/1)#switchport mode access
Device2(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device2(config-if-tengigabitethernet0/1)#exit
Device2(config)#interface tengigabitethernet 0/2
Device2(config-if-tengigabitethernet0/2)#switchport mode access
Device2(config-if-tengigabitethernet0/2)#switchport access vlan 3
Device2(config-if-tengigabitethernet0/2)#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 tengigabitethernet0/2 as trust port.

```
Device1(config)#dhcp-snooping
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device1(config-if-tengigabitethernet0/2)#exit
```

Step 5: Configure the port DAI function on Device1.

#Enable the port DAI function on port tengigabitethernet0/1.

```
Device1(config)#interface tengigabitethernet 0/1
```

```
Device1(config-if-tengigabitethernet0/1)#ip arp inspection
Device1(config-if-tengigabitethernet0/1)#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-if-vlan3)ip dhcp relay
Device2(config-if-vlan3)ip dhcp relay server-address 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     te0/1          107990         active
    ------
```

#PC2 can access IP Network normally and PC1 cannot access IP Network.

9.10 Host Guard

9.10.1 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:

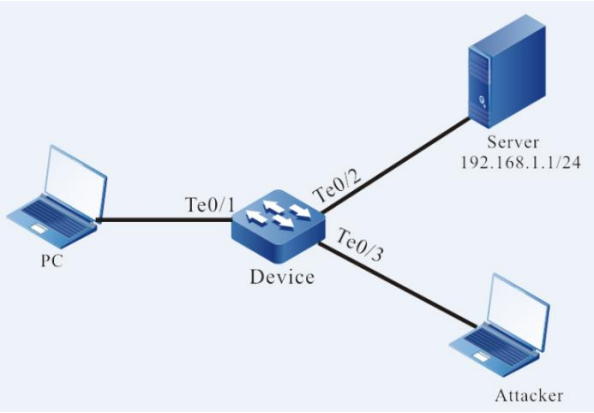


Figure 240 The brief diagram of the Host Guard function

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 te0/2, 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 te0/2, the packet can be processed normally; if the receiving port is not te0/2, the packet is dropped. That is, the ARP packet sent by Server can only be forwarded via port te0/2. The ARP packet forged by Attacker is dropped.

9.10.2 Host Guard Function Configuration

Table 1106 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

9.10.2.1 Configure Host Guard Function

Configuration Condition

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 1107 Configure the 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 1108 Configure the application of the 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		configuration mode, the subsequent configuration just takes effect on the aggregation group.
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.

9.10.2.2 Monitoring and Maintaining of Host Guard

Table 1109 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

9.11 AAA

9.11.1 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.

9.11.2 AAA Function Configuration

Table 1110 The configuration list of the AAA function

Configuration Task	
Configure the AAA domain	Configure ISP domain
Configure the authentication function in the AAA domain	Configure the default, login, dot1x and portal authentication methods in the ISP domain
Configure the authorization function in the AAA domain	Configure the default, login, and commands authorization methods in the ISP domain
Configure the accounting function in the AAA domain	Configure the default, login, dot1x, portal, and commands accounting methods in the ISP domain
Enter the authentication method of the privileged mode	Enter the authentication method of the privileged mode
Configure enabling the CLI authorization	Configure enabling the CLI authorization
	Configure enabling the Console authorization
Configure the system statistics function	Configure the statistics method of the system event
Configure the statistics attributes	Configure disabling the empty user name statistics
	Configure sending the statistics update packet
	Configure sending the statistics failure processing mode
Configure the RADIUS scheme	Configure the RADIUS server
	Configure the RADIUS attributes
	Configure the source address of sending the RADIUS packet
Configure the TACACS scheme	Configure the TACACS server
	Configure the source address of sending the TACAS packet

9.11.2.1 Configure the AAA Domain

Domain: NAS user management is based on ISP (Internet Service Provider) domain, and each user belongs to an ISP domain. In general, the ISP domain to which the user belongs is determined by the user name provided when the user logs in. There is a system domain by default. Under the domain, you can configure the authentication, authorization, and accounting method of each access user.

The solution of the domain-based user and AAA management is described as follows:

The management of NAS devices for users is based on the ISP domain. Generally, the ISP domain to which the user belongs is determined by the user name provided when the user logs in.

"Input User Name "= "User Name Understood by Device"+ "Domain Name"

When authenticating users, devices determine their domains in the following order, and then execute AAA policies in the domains:

1. (Optional) Log into/access the module to configure the designated authentication domain;
2. ISP domain specified in user name;
3. The default ISP domain of the system

Configuration Condition

None

Configure the ISP Domain

Table 1111 Configure the AAA domain

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ISP domain view	domain *isp-name*	Optional By default, the system has one

Step	Command	Description
		ISP domain named system.
Return to the global configuration mode	exit	-
Configure the default ISP domain	domain default enable *isp-name*	Optional By default, the default ISP domain of the system is the system domain.

9.11.2.2 Configure the Authentication Function in the AAA Domain

AAA provides a series of authentication methods to ensure the security of devices and network services. For example, authenticate user login to prevent illegal users from operating devices; authenticate users into privileged mode to restrict the using authorities of users for device; authenticate PPP session connections to restrict the setup of the illegal connections.

Configuration Condition

None

Configure the Authentication Method in the ISP Domain

AAA can authenticate a user when he tries to log into a specific ISP domain. Users who fail to authenticate cannot log into the specified ISP domain.

Table 1112 Configure the authentication method list in the ISP domain

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ISP domain view	domain *isp-name*	Mandatory By default, the system has one ISP domain named system.
Configure the default	aaa authentication default { none /	Optional

Step	Command	Description
authentication method in the ISP domain	local / radius-group *group-name* / tacacs-group *group-name* }	By default, the default authentication method in the ISP domain is local.
Configure the user login authentication method in the ISP domain	aaa authentication login { none / enable / local / radius-group *group-name* / tacacs-group *group-name* }	Optional By default, do not configure the login authentication method, but adopt the default authentication method in the domain.
Configure the portal|dot1x authentication method in the ISP domain	aaa authentication {portal | dot1x}{ none / local /radius-group *group-name* / tacacs -group *group-name* }	Optional By default, do not configure Portal, dot1x authentication method, but adopt the default authentication method in the domain.

9.11.2.3 Configure the Authorization Function in the AAA Domain

After successful authentication, the authorization function of AAA can control the rights of administrator users for device resources and access for network resources, restrict administrators to execute unauthorized commands, and restrict access users to access unauthorized network resources.

Configuration Condition

When configuring the command line authorization in the domain, first configure the authorization of enabling the command line so that the configured command line authorization in the domain can take effect.

Configure the Authorization Method in the ISP Domain

When a user executes an authorization item in a specific ISP domain, AAA can authorize the user, grant the user certain authorities, and prohibit the unauthorized user

to execute the authorization item in the domain.

Table 1113 Configure the authorization method list in the ISP domain

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ISP domain view	domain *isp-name*	Mandatory By default, the system has one ISP domain named system.
Configure the default authorization method in the ISP domain	aaa authorization default { if-authenticated / local / none / radius-group *group-name* / tacacs-group *group-name* }	Optional By default, the authorization method in the ISP domain is none.
Configure the commands authorization method in the ISP domain	aaa authorization commands *cmd-lvl* { if-authenticated / none / radius-group *group-name* / tacacs-group *group-name* }	Optional By default, do not configure the commands authorization method in the ISP domain, and the authorization method in the domain is none. The command authorization function must be enabled so that the configuration can take effect.
Configure the authorization method of the user logging into the device in the ISP domain	aaa authorization login { if-authenticated / local / none / radius-group *group-name* / tacacs-group *group-name* }	Optional By default, do not configure the login authorization method in the ISP domain, but adopt the default authorization method in the domain.

Note

- The **AAA** authorization commands and **aaa** authorization config-commands commands are configured in no sequence.

9.11.2.4 Configure the Accounting Function in the AAA Domain

The customized methods can be used to measure the command, login session, network service, and system events on the device. The statistical results can be used as the basis for charging users.

Configuration Condition

None

Configure the Accounting Method in the ISP Domain

When a user successfully logs into an ISP domain, AAA can count the user, including the start time of login, the end time of login, the commands entered, and so on.

Table 1114 Configure the accounting method in the ISP domain

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ISP domain view	domain *isp-name*	Mandatory By default, the system has one ISP domain named system.
Configure the command statistics method in the ISP domain	aaa accounting commands *cmd-lvl* { [broadcast] tacacs-group *group-name* }	Optional By default, do not configure the command statistics method, and do not

Step	Command	Description
		perform the command statistics.
Configure the default statistics method in the ISP domain	aaa accounting default { none | { start-stop | stop-only | wait-start [broadcast] { radius-group *group-name* / tacacs-group *group-name* }}}	Optional By default, the statistics method in the ISP domain is none.
Configure the accounting method of the user logging into the device in the ISP domain	aaa accounting login{ none | { start-stop | stop-only | wait-start [broadcast] { radius-group *group-name* / tacacs-group *group-name* } } }	Optional By default, do not configure the accounting method of the user logging into the device in the ISP domain, but use the default accounting method in the ISP domain.
Configure the portal|dot1x accounting method in the ISP domain	aaa accounting { portal | dot1x } { none | { start-stop | stop-only | wait-start [broadcast] { radius-group *group-name* / tacacs-group *group-name* } } }	Optional By default, do not configure the portal, dot1x accounting method in the ISP domain, but use the default accounting method in the ISP domain.

9.11.2.5 Enter the Authentication Method of the Privileged Mode

After the user successfully logs into the device, AAA can authenticate the user entering the privileged mode by entering the **enable** command, and prohibit the user entering the privileged mode if the authentication fails.

Configuration Condition

None

Configure the Authentication Method of the Privileged Mode

Table 1115 Configure the authentication method of the privileged mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the authentication method of the privileged mode	aaa authentication enable-method { none / enable / radius-group *group-name* / tacacs-group *group-name* }	Optional By default, the authentication method of the privileged mode is enable.

Note

- When using RADIUS authentication method, the password of the user name in the format of **$enabLEVEL$** is used as the authentication password, where LEVEL represents the user level entered by the current user, and the range of values is 0-15, and the highest level is 15.

9.11.2.6 Enable Command Authorization

Configuration Condition

None

Enable Command Authorization

The device has commands of 0 to 15 levels. Command authorization is to determine the level of commands used by users by authorization method, and restrict users to use the commands higher than the current level.

Table 1116 Enable the command authorization in the global mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the command authorization	aaa authorization config-commands	Mandatory By default, disable the command authorization function.

Enable Console Authorization

To perform the access restriction for the console port, you can enable Console port authorization, and need to enable the command authorization function. And then, the device will authorize the commands executed by console port.

Table 1117 Enable the Console authorization

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the Console authorization	aaa authorization console	Mandatory By default, do not enable the Console authorization.

9.11.2.7 Configure the System Event Statistics Function

Users can send events, such as system boot and reboot, to the server for statistics by configuring the system event statistics method.

Configuration Condition

None

Configure the System Event Statistics Method

Table 1118 Configure the system event statistics method list

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Configure the system event statistics method	aaa accounting system { none / { start-stop [broadcast] { tacacs-group *group-name* } } }	Mandatory By default, do not account the system events.

Note

- The system event statistics only supports the TACACS protocol, but does not support the RADIUS protocol.

9.11.2.8 Configure the Accounting Attributes

Configuration Condition

None

Disable Null-Username Accounting

The user can disable the AAA null-username accounting by configuring the command **aaa accounting suppress null-username**. By default, enable the AAA null-username accounting.

Table 1119 Disable the null-username accounting

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Disable the null-username accounting	aaa accounting suppress null-username	Mandatory By default, enable the null-username accounting.

Send Accounting Update Packet

The user can configure the mode of sending the accounting update packet, mainly including send in real time and send periodically.

Table 1120 Send the accounting update packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Send the accounting update packet	aaa accounting update periodic *interval*	Mandatory By default, do not send the accounting update packet.

Configure the Processing mode of Sending Accounting Failure

Table 1121 Send the processing mode of sending accounting failure

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the processing mode of sending accounting failure	aaa accounting start-fail {online | offline}	Optional By default, if the accounting starting fails, the user cannot get online.

9.11.2.9 Configure the RADIUS Scheme

To configure the RADIUS scheme, you need to configure the key parameters of the server.

Configuration Condition

None

Configure the RADIUS Server

When AAA needs to use the RADIUS method for authentication, authorization and accounting, it is necessary to configure RADIUS server parameters, including server IP address, authentication/authorization port, accounting port and shared key

information.

Before entering the RADIUS server, we need to configure the RADIUS server group. Reference the server group name when configuring the method list, and we can use the RADIUS server group to authenticate, authorize and count the users.

Table 1122 Configure the RADIUS server

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the RADIUS server group name (the command also can enter the RADIUS server group configuration mode)	aaa server group radius *group-name*	Mandatory By default, do not configure the RADIUS server group name.
Configure the RADIUS server	server {*ip-address*|*ipv6 ip-address*} [acc-port *acc-port-num*] [auth-port *auth-port-num*] [priority *priority*] { key [0 | 7] *key* }	Mandatory By default, do not configure the RADIUS server.
Configure the RADIUS dead time	dead-time *dead-time*	Optional By default, the dead time of the RADIUS server is 0, indicating not dead.
Configure the maximum re-transmit times of RADIUS	retransmit *retries*	Optional By default, the maximum re-transmit times of the RADIUS server is three times.
Configure the response timeout of the RADIUS server	timeout *timeout*	Optional By default, the timeout of waiting for the RADIUS server response is 5s.
Configure not checking TAG when resolving the	tunnel without-tag	Optional By default, need the TAG when

Step	Command	Description
tunnel attribute delivered by the RADIUS server		resolving the tunnel attribute delivered by the RADIUS server.
Configure the VRF of the RADIUS server group	ip vrf forwarding *vrf-name*	Optional By default, the RADIUS server group belongs to the global VRF.

Note

Devices select the order in which RADIUS servers are used according to the configured priority value.

Dead time means that the device marks the RADIUS servers that do not respond to authentication requests as unavailable and no requests are sent to these servers during dead-time.

The configured share keys on the device and RADIUS server must be consistent.

Configure the RADIUS Attributes

Table 1123 Configure the RADIUS attributes

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the attribute service-type value in the RADIUS packet of the login authentication	radius login service-type *attr-value*	Optional By default, the service-type value in the RADIUS packet is 7.
Configure the maximum concurrent packets of the NAS device and the RADIUS server	radius control-speed *pck-num*	Optional By default, the maximum concurrent packets of the NAS device and the RADIUS server is 100.

Configure the Source Address of Sending the RADIUS Packet

Table 1124 Configure the source address of sending the RADIUS packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the interface selected by the RADIUS source address	ip radius source-interface *interface-name* [vrf *vrf-name*]	Optional By default, the device automatically selects the source interface.

Configure the accounting-on Function of RADIUS

The account-on function is mainly used to designate all online users on the RADIUS server when the AAA process is pulled up for the first time. By default, the accounting-on function is disabled; when the account-on function is enabled, the default retransmit interval is 6 seconds, and the maximum retransmit times is 50 times; due to the slow start-up time of the service card of the high-end device, it is recommended that users set the retransmit times and the interval time not lower than the default values as far as possible.

Table 1125 Configure the accounting-on function of RADIUS

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the RADIUS server group mode	aaa server group radius *group-name*	-
Configure the account on function of RADIUS	accounting-on enable [interval *seconds* | send *send-times*]	Optional By default, the accounting-on function is disabled.

9.11.2.10 Configure the TACACS Scheme

To configure the TACACS scheme, it is necessary to configure the key parameters of the server.

Configuration Condition

None

Configure the TACACS Server

If AAA needs to use the TACACS method for authentication, authorization and accounting after configuring the TACACS server, it needs to configure the parameters of the TACACS server, including server IP address, shared key, server port number and other configuration information.

The TACACS server group can be used to authenticate, authorize and account users by referring to the server group name when configuring the method.

Table 1126 Configure the TACACS server

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the TACACS server group name (the command also can enter the TACAS server group configuration mode)	aaa server group tacacs *group-name*	Mandatory By default, do not configure the TACAS server group name.
Configure the TACACS server	server {*ip-address*|ipv6 *ip-address*} [port *port-num*] [priority *priority*] { key [0 | 7] *key*}	Mandatory By default, do not configure the member server of the TACAS server group.
Configure the response timeout of the TACAS	timeout *timeout*	Optional By default, the

Step	Command	Description
server		timeout of waiting for the TACAS server response is 5s.
Configure TACACS dead time	dead-time *dead-time*	Optional By default, the dead time of the TACACS server is 5, indicating 5 minutes.
Configure the VRF attribute of the TACAS server group	ip vrf forwarding *vrf-name*	Optional By default, the TACAS server group belongs to the global VRF.

Note

- You can execute the command **server** {*ip-address*|**ipv6** *ip-address*} [**port** *port-num*] [**priority** *priority*] { **key** [**0** | **7**] *key*} for many times to configure multiple TACAS servers in the Tacas server group. The device selects the server to authenticate according to the configuration order. When one server fails, the device automatically selects the next server.
- The configured share keys on the device and TACAS server must be consistent.

Configure the Source Address of Sending the TACAS Packet

Table 1127 Configure the source address of sending the TACAS packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Configure the interface selected by TACAS source address	ip tacacs source-interface *interface-name* [vrf *vrf-name*]	Optional By default, the device automatically selects the source interface.

9.11.2.11 AAA Monitoring and Maintaining

Table 1128 AAA monitoring and maintaining

Command	Description
debug aaa { authentication | authorization | accounting | event | error | all }	Enable the AAA debug information
debug radius [details]	Enable the RADIUS debug information
debug tacacs	Enable the TACAS debug information
show aaa configuration	Display the AAA configuration information
show aaa module [dot1x | shell | shell-cmd | shell-web | netconf]	Display the AAA function modules, and the result about the module operating AAA for the last time
show aaa server [radius | tacacs]	Display the RADIUS/TACACS server configuration and status of AAA
show aaa session [dot1x | portal | shell | shell-web]	Display the AAA statistics session
show aaa source-address	Display the source address used by AAA

9.11.3 AAA Typical Configuration Example

9.11.3.1 Configure Telnet User Login to Use Local Authentication

Network Requirement

Configure Device to use local authentication for Telnet user login

Network Topology

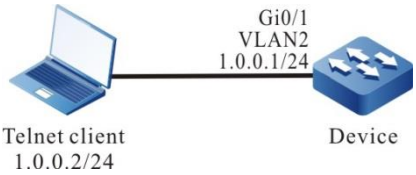


Figure 241 Networking of configuring Telnet user login to use local authentication

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 admin1 and password as admin1.

```
Device#configure terminal
Device(config)#local-user admin1 class manager
Device(config-user-manager-admin1)#service-type telnet
Device(config-user-manager-admin1)#password 0 admin1
Device(config-user-manager-admin1)#exit
```

#Configure the AAA authentication mode as the local authentication.

```
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#exit
```

#Configure the Telnet session and enable the AAA local authentication.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
Device(config-line)#exit
```

Step 4: Check the result.

When the client logs in to Device via Telnet, input the user name admin1 and password admin1 according to the prompt, and then log in to the Shell user interface of Device successfully.

9.11.3.2 Configure Telnet User Login to Use RADIUS Authentication, Authorization and Statistics

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

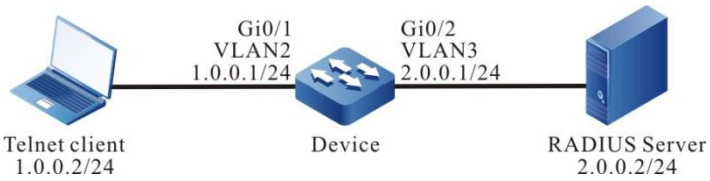


Figure 242 Networking of configuring Telnet user login to use RADIUS authentication/authorization and accounting

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/authorizationm and accounting.

Note

- Authentication and authorization first use the first method in the method list. Use the second method to authenticate and authorize when the server fails.

```
Device#configure terminal
Device(config)#domain system
Device(config-isp-system)#aaa authentication login radius-group radius-group local
Device(config-isp-system)#aaa authorization login radius-group radius-group local
Device(config-isp-system)#aaa accounting login start-stop radius-group radius-group
Device(config-isp-system)#exit
```

#Configure the RADIUS server, the authentication port is 1812, the statistics port is 1813, and the share key is admin.

```
Device(config)#aaa server group radius radius-group
Device(config-sg-radius-radius-group)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
Device(config-sg-radius-radius-group)#exit
```

#Configure the Telnet session and enable the RADIUS authentication/authorization and statistics.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
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 statistics 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 statistics.

#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.

9.11.3.3 Configure Telnet User Level Switching to Use RADIUS Authentication

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

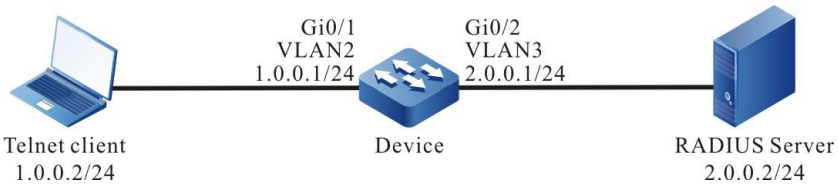


Figure 243 Networking of configuring Telnet user level switching to use RADIUS authentication

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#configure terminal
Device(config)#aaa authentication enable-method radius-group radius-group
Device(config)#domain system
Device(config-isp-system)#aaa authentication login radius-group radius-group local
Device(config-isp-system)#exit
```

#Configure the RADIUS server, the authentication port is 1812, and the share key is admin.

```
Device(config)#aaa server group radius radius-group
Device(config-sg-radius-radius-group)#server 2.0.0.2 auth-port 1812 acct-port 1813 key admin
Device(config-sg-radius-radius-group)#exit
Device(config)#line vty 0 15
Device(config-line)#login aaa
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 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.

9.11.3.4 Configure TACACS Authorization and Statistics of Shell Command

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

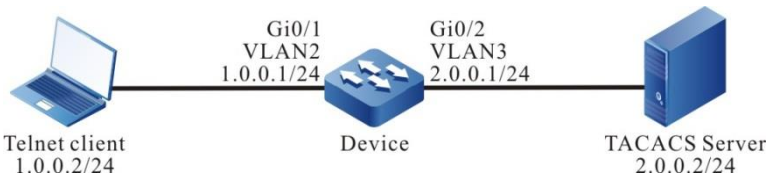


Figure 244 Networking of configuring the TACACS authorization and accounting of the Shell command

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

- The authentication should succeed before authorization and accounting.

```
Device#configure terminal
Device(config)#domain system
Device(config-isp-system)#aaa authentication login tacacs-group tacacs-group local
Device(config-isp-system)#aaa authorization commands 15 tacacs-group tacacs-group
Device(config-isp-system)#aaa accounting commands 15 tacacs-group tacacs-group
Device(config-isp-system)#exit
Device(config)#aaa authorization config-commands
```

#Configure the TACACS server, the service port is 49, and the share key is admin.

```
Device(config)#aaa server group tacacs tacacs-group
Device(config-sg-tacacs-tacacs-group)#server 2.0.0.2 port 49  key admin
Device(config-sg-tacacs-tacacs-group)#exit
```

#Configure the Telnet session and enable the TACACS authorization and accounting.

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
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 fastethernet 0/1
Command authorization failed
Device(config)#router bgp 100
Command authorization failed
```

#View the Shell command statistics information.

On the TACACS server, we can see the statistics information of the Shell command.

9.12802.1X

9.12.1 Overview

9.12.1.1 802.1X

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).

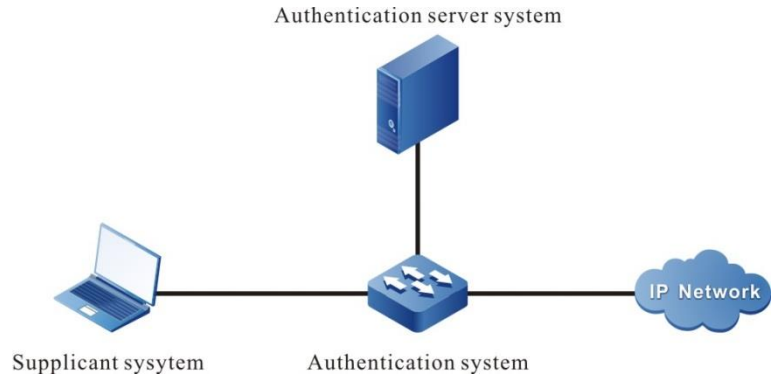


Figure 245 802.1X system architecture

- 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:

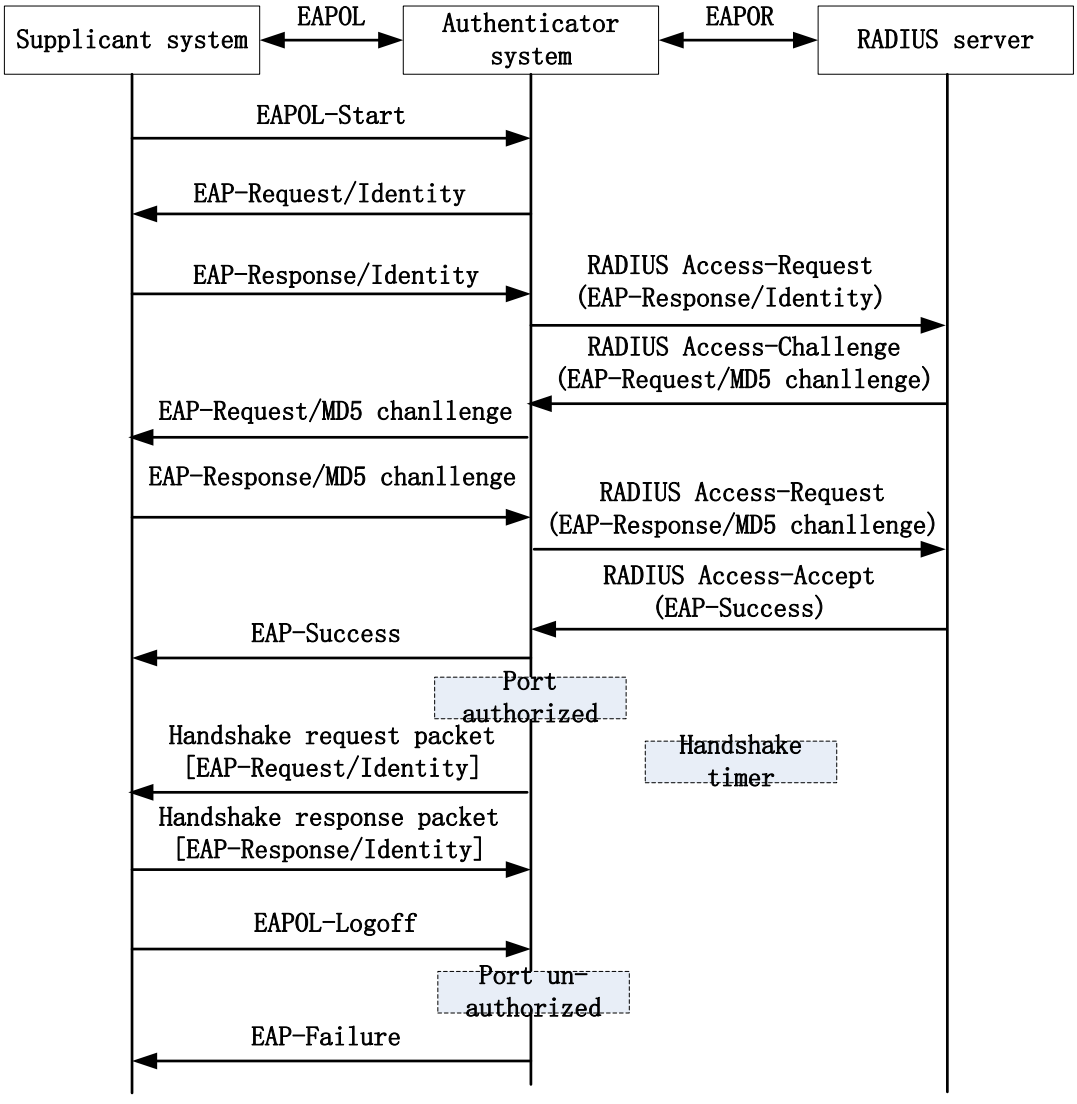


Figure 246 802.1X relay authentication flow

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:

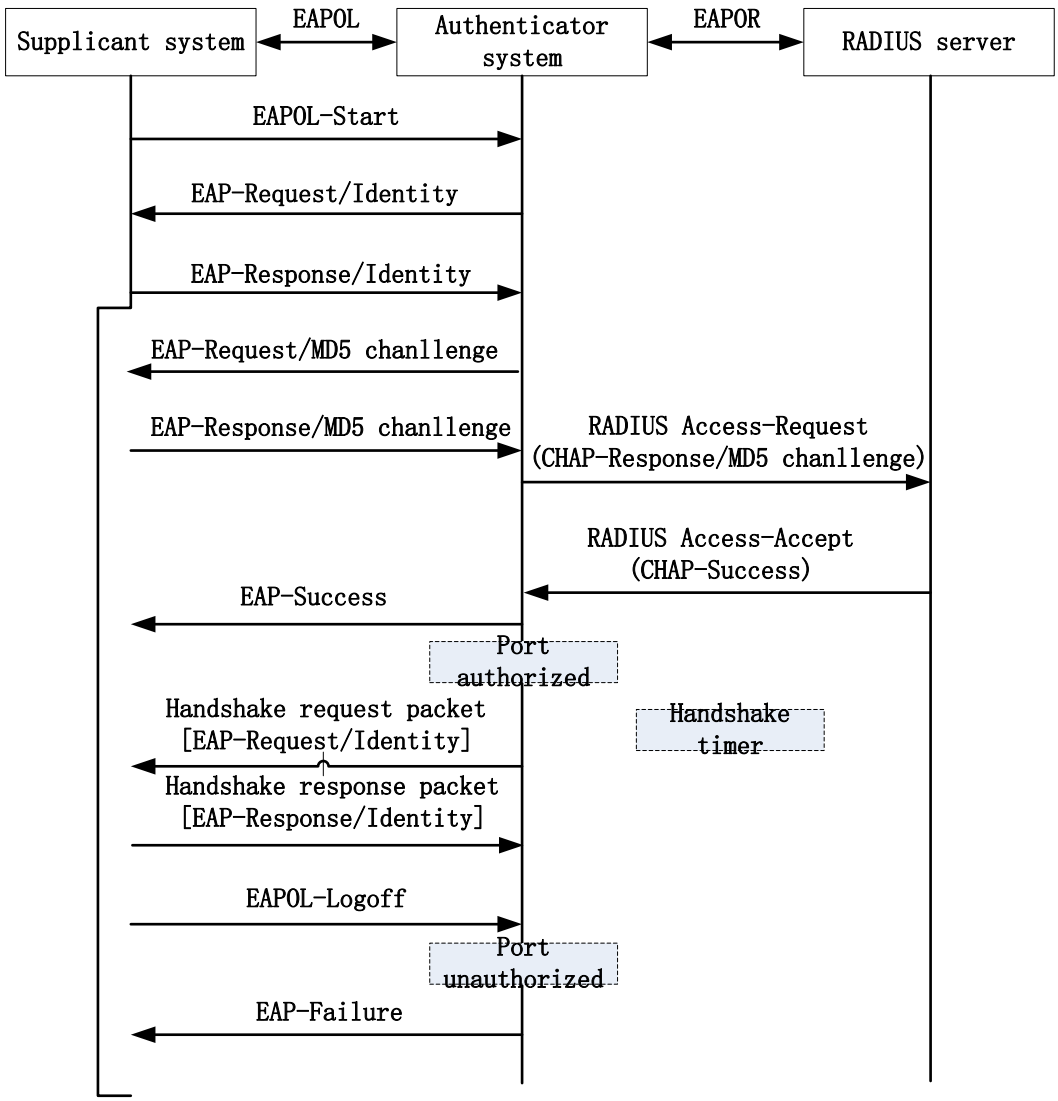


Figure 247 802.1X terminating authentication flow

- 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 is restored to the un-authenticated state, the port is deleted from the Auto VLAN , and the default value of the port is restored to the previous configured VLAN.
- After enabling Guest VLAN, the user 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 802.1x authentication and properly configuring the guest VLAN, the port will be added to the guest VLAN in the untagged mode. At this time, the user under the port in the guest VLAN initiates authentication. If the authentication fails, the port is still in the guest VLAN. If the authentication is successful, it can be divided into the following two cases:

- If the authentication server delivers a VLAN, the port leaves the guest VLAN and joins the distributed VLAN. After the user is offline, the port will return to the guest VLAN;
- If the authentication server does not deliver VLAN, the port leaves the guest VLAN and joins the configured config VLAN in the authentication device. After the user is offline, the port will return to the guest VLAN.

9.12.1.2 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.

9.12.1.3 MAC Address Authentication

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.

9.12.2 802.1X Function Configuration

Table 1129 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 the function of omitting the IP field in the user name
	Configure the packet transparent-transmission function
	Configure the keepalive 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

Configuration Task	
	user name format
	Configure the domain name used by the MAC authentication globally
	Configure not to enter the guest-vlan function after MAC authentication failed
Configure the public attributes	Configure the controlled direction
	Configure the authenticable host list
	Configure the IP authorization function
	Configure the maximum sending times of the authentication request packet
	Configure the maximum sending times of the authentication packet
	Configure the record data log function
	Configure the ARP keepalive function
	Configure the maximum users of the port
	Configure the IP ACL prefix name
	Configure the default valid VLAN
	Configure permitting the unauthenticated user to communicate in the belonging VLAN of the PVID
	Configure the port access control mode
	Configure Guest VLAN
	Configure Guest ACL
	Configure Critical VLAN
	Configure the user authentication move function
	Configure the timer parameters
	Restore the default configuration of the port
	Configure the log record step
	Configure none escape user to re-authenticate
	Configure the uplink port of the user speed limit

9.12.2.1 Configure 802.1X Authentication Function

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 Condition

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 1130 Enable 802.1X

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enable global 802.1X authentication	dot1x { enable | disable }	Optional By default, the global 802.1X authentication function is enabled.
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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enable the 802.1X authentication	dot1x port-control { enable | disable }	Mandatory By default, the 802.1X authentication function in the port is disabled.

Note

- Do not enable the 802.1X authentication function and secure channel authentication function simultaneously on one port.
- Support enabling the 802.1X authentication function and port security function on one port at the same time, but there is the following limitation: Do not permit configuring the port security IP rule or MAX rule.
- If the port security is configured with the related MAC rule when 802.1X authentication function is used with the port security function, 802.1X does not process the sent packets and authentication requests of the terminal, which are processed by the port security.

Configure the ARP/IP Packet to Trigger Generating the 802.1X User

After enabling 802.1X authentication function on the port, if the terminal user wants to view the information of the terminal user on the authentication device without initiating authentication, it needs to configure the ARP/IP packet to trigger generating 802.1X user.

Enable the 802.1X authentication function, and the function of the ARP/IP packet

triggering generating the 802.1X user on one port. When the authentication device receives the ARP or IP packet of the terminal user in the port, it can generate the 802.1X user.

Table 1131 Enable the function of the ARP/IP packet triggering generating the 802.1X user

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	interface link-aggregation *link-aggregation-id*	
Configure the function of the ARP/IP packet triggering generating the 802.1X user	dot1x arp-ip-auth { enable | disable }	Mandatory By default, the function of the ARP/IP packet triggering generating the 802.1X user is disabled on the port.
Configure the timeout of the ARP/IP packet triggering generating the 802.1X user	dot1x arp-ip-auth timeout *timeout-value*	Optional By default, the timeout of the ARP/IP packet triggering generating the 802.1X user is 5 minutes.

9.12.2.2 Configure Secure Channel Authentication

Configuration Condition

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 1132 Enable the 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	interface 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

- Do not enable the secure channel authentication function and port security function simultaneously on one port.

- 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.

Configure and Apply Secure Channel

After the secure channel authentication is enabled under the interface, it is hoped that the end user can visit the resources in the specified network when the end user is not authenticated or specify an end user to visit the network resources without authentication. In this case, configure and apply the secure channel.

Rules for configuring the secure channel can be classified into the following types:

- Configure to allow the end user to visit the specified network resources.
- Configure the specified end user to visit the network resources.

Table 1133 Apply secure channel

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the secure channel	hybrid access-list advanced { *access-list-number* | *access-list-name* }	Mandatory By default, the secure channel is not configured on the device.
Configure the secure channel	[*sequence*] permit [ether-ipv6]	Mandatory

Step	Command	Description
rule	*protocol* { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any | *source-mac-addr source-wildcard* | host *source-mac-addr* } { any | *destination-ip-addr destination-wildcard* | host *destination-ip-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* }	By default, the secure channel rule is not configured in the secure channel.
Apply the secure channel	global security access-group { *access-group-number* | *access-group-name* }	Mandatory By default, no any secure channel is applied in the system.

Note

- The device can be configured with multiple secure channels. A secure channel can be configured with multiple secure channel rules.
- The secure channel type can only be the hybrid advanced ACL. Only one secure channel is allowed to be applied to the device.

Configure Re-direct URL Function

If the re-direct URL is configured on the authentication device and when the user accesses the segment network not free from the authentication without passing the authentication or not being authenticated, the authentication device re-direct the user accessed URL address to the configured re-direct URL address. On the specified URL interface, the user can download/upgrade the authentication client, update the software, and so on.

Table 1134 Configure the re-direct URL function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the secure channel	hybrid access-list advanced { *access-list-number* | *access-list-name* }	Mandatory By default, the device is not configured with the secure channel.
Configure the secure channel rule	[*sequence*] permit [ether-ipv6] *protocol* { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any | *source-mac-addr source-wildcard* | host *source-mac-addr* } { any | *destination-ip-addr destination-wildcard* | host *destination-ip-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* }	Mandatory By default, the secure channel is not configured with the secure channel rule.
Apply the secure channel	global security access-group { *access-group-number* | *access-group-name* }	Mandatory By default, no secure channel is applied in the system.
Configure the re-direct URL function	dot1x url *url-redirect-string*	Mandatory By default, the re-direct URL address is not configured on the device.

Note

- The segment free from the authentication needs to include the IP address of the DNS server and the IP address of the re-direct URL link.
- When the client needs to apply for address from the DHCP server, and the

authentication device is not the DHCP server, it is necessary to enable the DHCP RELAY function on the authentication device, so as to ensure that the client can get the IP address normally.

9.12.2.3 Configure 802.1X Authentication and Secure Channel Authentication Property

If the 802.1X authentication function or the secure channel authentication function is not enabled on the interface, then the configured 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 1135 Configure the 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	interface link-aggregation *link-aggregation-id*	
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.

- When the client adopts the certificate authentication, the authentication port needs to be configured as the relay 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 1136 Configure the 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	interface link-aggregation *link-aggregation-id*	
Enable the multicast trigger	dot1x multicast-trigger	Mandatory By default, the multicast trigger function in the port is disabled.

Step	Command	Description
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 1137 Configure the 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		group.
Configure the re-authentication	dot1x reauthentication	Mandatory 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 1138 Configure the 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	interface 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 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 1139 Configure the 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	interface 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.
Configure the uplink port	dot1x eapol-relay uplink { interface *interface-name* | link-	Mandatory By default, the port is not

Step	Command	Description
	aggregation *link-aggregation-id* }	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 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 1140 Configure the 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	interface 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-	dot1x keepalive retries *retries-*	Optional

Step	Command	Description
transmitting the keepalive packet	*value*	By default, the maximum keepalive time in the port is 3.
Configure the keepliave type	dot1x keepalive type { request-identity | request-md5}	Optional By default, the keepalive type in the port is the standard keeplive.

Note

- The keepalive function needs to be supported by the 802.1X authentication client software (such as Sofinet TC client). If the client does not support, it may result in the keepalive failure and the user gets offline.

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 1141 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		configuration just takes effect on the aggregation group.
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.

9.12.2.4 Configure MAC Address Authentication

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 Condition

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 1142 Enable the 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 the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
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

- Support enabling the MAC address authentication function and port security function on one port at the same time, but there is limitation: do not permit configuring the port security IP rule or MAX rule.
- Do not enable the MAC address authentication function and security 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 01-01-7a-00-00-01; the other is not with hyphen, such as 01017a000001.

Table 1143 Configure the 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 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	interface link-aggregation *link-aggregation-id*	
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.

Configure Domain Name Used by MAC Authentication in Global Mode

This function can be enabled when MAC authenticated users accessed by all ports

on the device need to be forcibly assigned to a specified domain for authentication.

By default, the domain name used for MAC authentication is not specified globally. The domain used for user authentication uses the mandatory authentication domain configured by the port. If the port is not configured with the mandatory authentication domain, use the domain carried by the user name. If the user does not carry the domain, use the default domain of the AAA module.

After being configured on the port, the priority of the domain used by the MAC authenticated user accessed by the port is: the mandatory authentication domain configured on the port > the domain carried by the fixed user name configured on the port > globally specify the domain used for MAC authentication > the default domain of AAA module; The priority of the domain used by 1x authenticated user accessed under the port is: mandatory authentication domain configured by the port > domain carried by the user > default domain of AAA module.

Table 1144 Configure the domain name used by the MAC authentication in global mode

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the domain name function used by MAC authentication in global mode	dot1x mac-authentication domain *domain-name*	Mandatory By default, do not configure the domain name function used by MAC authentication in global mode.

Configure Domain Name Delimiter

The authentication device can manage the user based on the domain. If the authentication user name carries the domain name, the device uses the server in the AAA server group to authenticate, authorize and account the user. If the authentication user name does not carry the domain name, use the default configured authentication server in the system to authenticate. Therefore, the authentication device needs to parse the user name and domain name correctly, playing the decisive function for the user to

provide the authentication service. Different clients support different user name and domain name delimiters. To manage and control the user access of different user name formats better, it is necessary to specify the supported domain name delimiter on the authentication device.

Currently, the supported domain name delimiters include @, /, and \.

When the domain name delimiter is @, the authenticated user name format is username@domain.

When the domain name delimiter is /, the authenticated user name format is username/domain.

When the domain name delimiter is \, the authenticated user name format is domain\username.

Here, username is the pure user name, and domain is the domain name. If the user name contains multiple domain name delimiters, the authentication device only identifies the first domain name delimiter as the actual used domain name delimiter and the other characters as one part of the domain name.

Table 1145 Configure the domain name delimiter

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	**interface link-aggregation** *link-aggregation-id*	

Step	Command	Description
Configure the domain name delimiter	**dot1x domain-delimiter** *domain-delimiter-type*	Mandatory By default, the domain name delimiter in the port is @.

Note

- When using the user name with the domain name to authenticate, it is necessary to configure the corresponding authentication server group on the authentication device.

Configure Authentication User Name Format

The authentication user is named by the format of username@domain. The domain name is behind the domain name delimiter @. The authentication device decides which authentication server group authenticates the user by parsing the domain name. The early server cannot accept the user name with the domain name, so the authentication device needs to delete the domain name carried in the user name and just send the authentication user name to the server. You can select whether the authentication user name sent to the authentication device carries the domain name by configuring the format of the authentication user name.

Currently, the supported domain name delimiter includes @, \, /.

Table 1146 Configure the 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 current
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		port. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure the format of the authentication user name	dot1x user-name-format { with-domain | without-domain }	Mandatory By default, send the authentication user name with the domain name to the authentication server.

Note

- Configure the port of sending the authentication user name without domain name to the authentication server not to support the certificate authentication.

Configure Interacting Mode of Authentication Packet

In the actual application scenario, after most of clients initiate the authentication, the authentication device and client support unicast/multicast authentication interacting mode, but there are still come authentication clients that can only identify the multicast authentication packet, that is, the authentication packet with the destination MAC address 0180.C200.0003. Here, you can configure the multicast authentication interacting mode in the port.

For most of authentication clients, after the authentication device receives the EAP packet responded by the server for the first time and interacts with the client and authentication server, be subject to the identifier in the service packet. Only a few of authentication clients need to be subject to the identifier generated by the authentication device. As for the case, it is necessary to configure the function of concerning the

identifier in the EAP authentication packet in the port.

Table 1147 Configure the interacting mode of the authentication 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	interface link-aggregation *link-aggregation-id*	
Configure the authentication interacting mode	dot1x auth-mac { multicast | unicast }	Mandatory By default, the port adopts the interacting mode of the unicast authentication packet.
Concern the identifier in the EAP authentication packet	dot1x identifier { match | ignore }	Optional By default, do not concern the identifier in the EAP authentication packet.

Note

- Only a few of clients need to concern the identifier of the authentication interacted packet. Unless there is a clear demand, try to avoid configuring the function.

Configure the Function of Not Entering guest-vlan after MAC Authentication Failed

After enabling the function of not entering guest-vlan after MAC authentication failure, when the guest VLAN function is configured, the user with MAC authentication failure will not enter guest-vlan, and the user with 802.1x authentication failure will enter the guest-vlan; If the function of not entering guest-vlan after MAC authentication failure is disabled, the users with MAC authentication and 802.1x authentication failure will enter the guest-vlan.

Table 1148 Configure the function of not entering guest-vlan after MAC authentication failure

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	interface link-aggregation *link-aggregation-id*	
Configure the function of not entering guest-vlan after MAC authentication failure	dot1x mac-authfail guest-vlan exclude	Mandatory By default, the port does not enable the function of not entering guest-vlan after MAC authentication failure.

9.12.2.5 Configure Public Attributes

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 Condition

When configuring the IP authorization function on the port, you need to configure the ARP keepalive function at the same time.

Configure Controlled Direction

The controlled direction of the port includes bi-directional controlled and uni-directional controlled.

- Bi-directional controlled: The port prohibits receiving and forwarding packets.
- Uni-directional controlled: Prohibit receiving client packets, but permit forwarding packets to the client.

The function is used with the WOL (Wake On Lan) function. Some terminal is in the dormant state, but its network card still can process some special packets, such as WOL packets. After the network card receives the WOL packets, enable the terminal device and enter the working state.

When the access port of the dormant terminal enables the authentication function, you can configure the port as the uni-directional controlled, ensuring that the WOL packets can be forwarded to the terminal normally. After the terminal starts, it can initiate the authentication. After passing the authentication, it can access the network resources normally.

When sending the WOL packets across the segment, it is necessary to configure the ARP forwarding entry on the authentication device.

Table 1149 Configure the controlled direction

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,

Step	Command	Description
		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.
Configure the controlled direction	dot1x control-direction { both | in }	Mandatory By default, the port is controlled bi-directionally.

Configure Authenticable Host List

After enabling the authenticable host list function, only permit the user whose MAC address is in the authenticable host list to authenticate and the authentications initiated by the other users are refused.

Table 1150 Configure the authenticable host list

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 configuration just takes effect on the aggregation

Step	Command	Description
		group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the authenticable host list	dot1x auth-address { enable | disable | *mac-address* }	Mandatory By default, the authenticable host list under the port is disabled.

Configure IP Authorization Function

When enabling the IP authorization function on the port and if finding that the IP address of the authentication user changes, force the user offline, including the following modes:

Disable: In the mode, do not detect the IP address of the user.

dhcp-server: When configuring the mode, it is necessary to configure the DHCP Snooping function on the device. After the authentication user gets the IP address from the DHCP server, record the binding relation of the authentication user and IP address on the device. If finding that the IP address of the user changes, force the user offline.

radius-server: RADIUS Server encapsulates the IP address used encapsulating the authentication user in the Frame-IP-Address field in the RADIUS packet and the authentication device records the binding relation of the user and the IP address. If finding that the user IP address changes, force the user offline.

Supplicant: After the user passes the first authentication, the device records the binding relation of the authentication user and IP address. If finding that the user IP address changes, force the user offline.

bind-mac-ip: MAC+IP binding mode, after the authentication user passes the first authentication, a MAC + IP binding entry will be generated and the entry configuration will be saved. Later, only the IP address in the binding entries generated when the first authentication is passed can be used to access the network.

Table 1151 Configure the IP authorization 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 configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the IP authorization function	dot1x authorization ip-auth-mode { disable | dhcp-server | radius-server | supplicant | bind-mac-ip }	Mandatory By default, the IP authorization function is disabled on the port.

Configure Max. Sending Times of Authentication Request Packets

After the authentication device receives the EAPOL-Start packets sent by the client, send the authentication request EAP-Request/Identity packet to the client. If the authentication device does not receive the response packet, re-transmit the packet. The function is used to configure the maximum sending times of the EAP-Request/Identity packet. If the sending times exceeds the configured maximum value, the authentication device judges that the client is disconnected and ends the authentication.

The process of re-transmitting the EAP-Request/Identity packet is as follows:

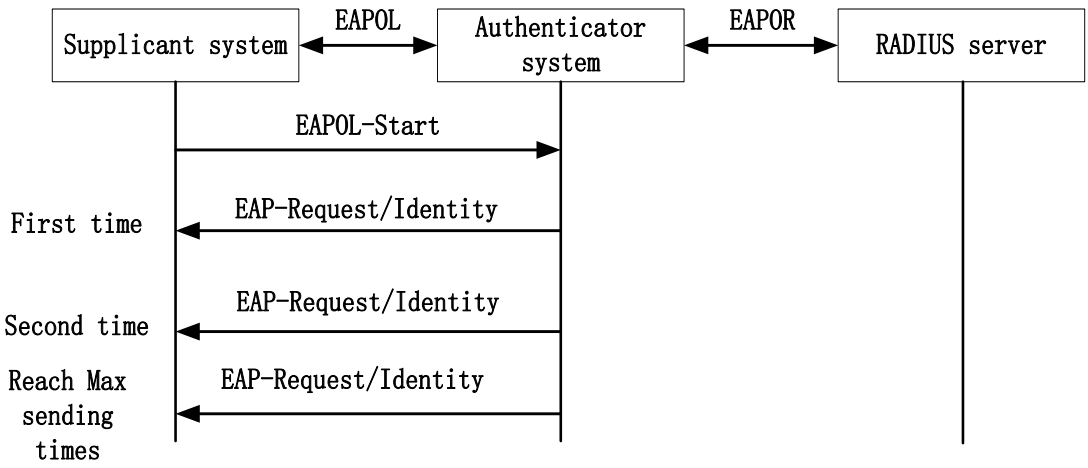


Figure 248 Re-transmit EAP-Request/identity packets

Table 1152 Configure the maximum sending times of the authentication request packets

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 configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the maximum sending times of the authentication request packets	dot1x max-reauth *count*	Mandatory By default, the maximum sending times of the authentication request packet

Step	Command	Description
		on the port is 3.

Configure Max. Sending Times of Authentication Packet

During the authentication, the authentication device sends the other EAP-Request packets except for EAP-Request/Identity packets to the client, such as EAP-Requesst/MD5 chanllenge packet. If the authentication device does not receive the response packet, re-transmit the packet. The function is used to configure the maximum sending times of the packet. If the sending times exceeds the configured maximum value, the authentication device judges that the client authentication fails.

The process of re-transmitting the EAP-Request packet is as follows:

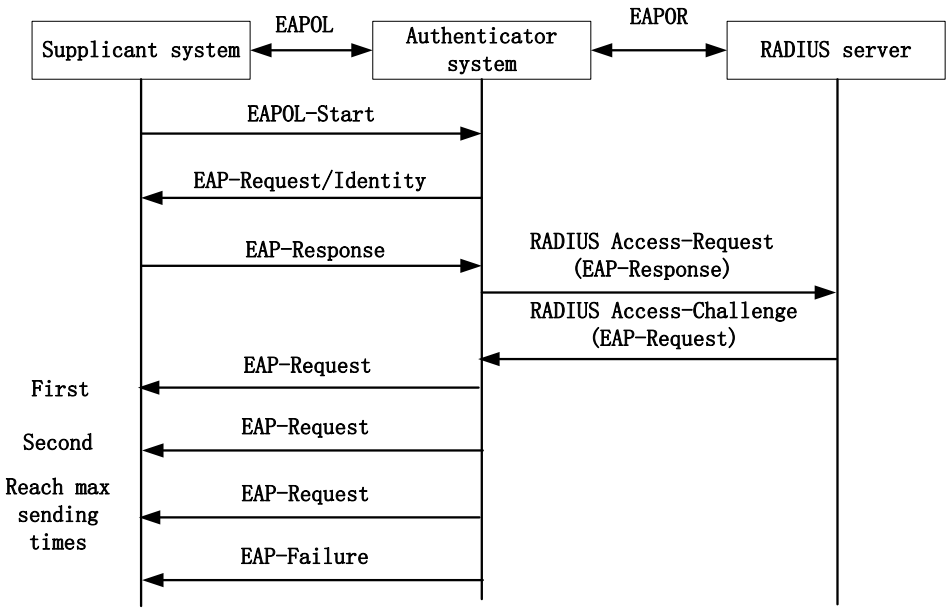


Figure 249 Re-transmit the EAP-Request packet

Table 1153 Configure the maximum sending times of the authentication 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

Step	Command	Description
		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.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Configure the maximum sending times of the authentication packet	dot1x max-req *count*	Mandatory By default, the maximum sending times of the authentication packet on the port is 2.

Configure Record Data Log Function

After enabling the record data log function, the authentication device will record the information about the user online/offline and user information change, so as to detect the fault reason.

Table 1154 Configure the record data 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure recording data log function	dot1x logging security-data {abnormal-logoff | failed-login | normal-logoff | successful-login | information}*	Mandatory By default, the function of recording data log is not enabled on the port.

Configure ARP Keepalive Function

To check whether the user is online after the terminal user passes the authentication, the authentication device sends the ARP request packets to the authenticated user. The authentication device confirms whether the user is online by whether receiving the ARP response packet of the user.

Table 1155 Configure the 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 interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
Configure the ARP keepalive function	dot1x client-probe { enable | disable }	Mandatory By default, the ARP keepalive function under the port is disabled.

Note

- The authentication device can trigger ARP keepalive function normally only after getting the authenticated user IP address. If not receiving the ARP response packet of the authentication device during the protection period, force the user offline.

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 1156 Configure the maximum users of 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	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
Configure the maximum users of the port	authentication 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 1157 Configure the 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-".

Note

- When the access control mode is configured as port-based multi-host mode (portbased host-mode multi-hosts), delivering the ACL function does not take effect.

Configure Default Valid VLAN

When 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.

Table 1158 Configure the 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

- 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.
- When the port is configured based on the user access control mode (macbased), the default effective VLAN will take effect when the port meets the VLAN mode of hybrid mode and MAC VLAN condition is enabled.

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).
- Port VLAN mode is Hybrid mode.
- The function of only receiving the Untag packet needs to be enabled on the interface.

Table 1159 Configure to allow the unauthenticated user to communicate in the VLAN which the 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 receiving 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.
- The function does not support the secure channel authentication.

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 1160 Configure the 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		takes effect on the aggregation group.
Configure the access control mode	authentication port-method { macbased | portbased }	Mandatory By default, enable the user authentication mode in the port.
Configure the port-based access control mode	authentication 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 1161 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		takes effect on the aggregation group.
Configure Guest VLAN	authentication 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 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 1162 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		configuration mode, the subsequent configuration just takes effect on the aggregation group.
Configure Guest ACL	authentication 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.
- Guest ACL can take effect only in the user-based access control mode (Macbased).
- The ACL rule is configured in the authentication device.

Configure Critical VLAN

When the user adopts the RADIUS authentication, the authentication server is not available and as a result, the authentication fails. Permit the user to access the resources in the specified VLAN and the VLAN is called Critical VLAN.

When the port is configured as the port-based access control mode and there is user to authenticate on the port, but all authentication servers are not available, the port is added to Critical VLAN and all users under the port can access the resources in the Critical VLAN.

When the port is configured as user-based access control mode and there is user to authenticate on the port, but all authentication servers are not available, the user is only permitted to access the resources in Critical VLAN.

If the port is configured as the user-based access control mode, it should meet the following conditions to run normally:

- Port VLAN mode is Hybrid mode
- The port enables the MAC VLAN function. The user in the Critical VLAN initiates the authentication. If the authentication server is still not available, the user is still in Critical VLAN. If the authentication server is available, the user exits Critical VLAN with the authentication result.

After the port is added to Critical VLAN and if the authentication device is configured with the AAA detection function, it is detected that the authentication server is available. If critical-vlan recovery reinitialize is configured:

- If the port is mac-based access control mode, the port added to Critical VLAN will send the unicast packet to all users in Critical VLAN actively, triggering the user to re-authenticate.
- If the port is port-based access control mode, the port added to Critical VLAN will actively send the multicast packet, triggering the user to re-authenticate.

Table 1163 Configure Critical 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	interface link-aggregation *link-aggregation-id*	
Configure Critical VLAN	authentication critical-vlan *critical-vlan-id*	Mandatory By default, do not configure

Step	Command	Description
		Critical VLAN under the port. The value range is 1-4094.
Configure port recovery and trigger authentication	authentication critical-vlan recovery-action reinitialize	Optional By default, after the authentication server is detected to be available, the port only leaves Critical VLAN.

Note

- The function only supports the RADIUS authentication.
- If the radius and escape function are configured on the device, that is, configure **aaa authentication dot1x radius none** and **critical vlan**, when the user authenticates, the authentication server is not available and the user will not enter the Critical VLAN, but escape directly. If only escape function is configured, that is, configure **aaa authentication dot1x none** and **critical vlan**, when the user authenticates, the escape function takes effect.
- When only configuring the Guest VLAN function under the port, the user failed to authenticate is in Guest VLAN. When Guest VLAN and Critical VLAN function are configured under the port at the same time, the user fails to authenticate because the authentication server is not available and enters Critical VLAN. If the user fails because of other reason, it enters Guest VLAN.
- For AAA detection function, refer to the configuration of Section AAA.

Configure User Authentication Transfer Function

The user authentication transferring function applies to the scenario where the same user (distinguish based on terminal MAC address) transfers from one

authentication port of the same device to another. When the user authentication transferring function is disabled, the user is not allowed to initiate authentication on another authentication port of the device after being authenticated on one port of the device; when the user authentication transferring function is enabled, and after the user is authenticated on one port, the device first deletes the authentication information on the original port after detecting that the user transfers to another authentication port, and then, allows the user to initiate authentication on the new authentication port

Whether or not user authentication transferring function is enabled, the device will record the log when detecting that the user transfers between the authentication ports.

Table 1164 Configure the user authentication transferring 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	interface link-aggregation *link-aggregation-id*	
Configure the user authentication transferring function	authentication station-move { enable | disable }	Mandatory By default, the user authentication transferring function is disabled.

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 1165 Configure the 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

Step	Command	Description
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	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 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 300s; the value range is 5-3600;

Configure MAB Function

When the terminal passes MAC address authentication and needs to pass client authentication to use higher access rights, this function can be enabled.

Table 1166 Enable the MAB function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the L2 Ethernet interface	interface *interface-name*	Either

Step	Command	Description
configuration mode		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	interface link-aggregation *link-aggregation-id*	
Enable the 802.1X authentication	dot1x port-control { enable | disable }	Mandatory By default, the 802.1X authentication function is disabled in the port.
Enable the MAC address authentication function	dot1x mac-authentication { enable | disable }	Mandatory By default, the MAC address authentication function is disabled on the port.
Enable the MAB function	dot1x after-mac-auth { enable | disable }	Mandatory By default, the MAB function is disabled on the port.

Restore Port Default Configuration

Restore the default configuration of the 802.1X authentication and MAC address authentication in the port.

Table 1167 Restore the default configuration of 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,
Enter the aggregation group	interface link-aggregation *link-*	

Step	Command	Description
configuration mode	*aggregation-id*	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.
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 Port Forced Authentication Domain Function

You can enable this function when you need to forcibly assign the authenticated users on the port to a specified domain for authentication.

By default, the port mandatory authentication domain is not configured. The domain used for user authentication uses the domain carried by the user name. If the user does not carry the domain, the default domain of the aaa module is used.

After the configuration on the port, the priority of the domain used by the user is: domain configured under the port > domain carried by the user > default domain of the

aaa module.

Table 1168 Enable forced authentication domain 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	interface link-aggregation *link-aggregation-id*	
Enable 802.1X forced authentication domain function	dot1x authentication domain *domain-name*	Mandatory By default, do not configure the forced authentication domain in the port.

Configure None Scape User Re-authentication Function

In the actual application scenario, the network fluctuates and the aaa server in the user authentication domain is blocked. At this time, the authenticated user adopts the aaa none escape. After the server becomes available, if the escape user needs to be authenticated again, this function can be enabled. This function needs to be combined with the server detection function of aaa.

By default, none escape user re-authentication function is not enabled.

Table 1169 Enable none scape user re-authentication function

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	interface link-aggregation *link-aggregation-id*	
Enable none scape user re-authentication function	dot1x escape-user re-auth	Mandatory By default, do not configure the none scape user re-authentication function in the port.

Configure the Uplink Port of User Speed Limit

In the scenario where the user-based egress speed limit is distributed through the server, if the device does not support egress ACL, we need to configure this function. If the device supports the egress ACL, this configuration is ignored, and we do not need to configure this function.

When the device does not support the egress ACL, the user authenticates successfully and distributes the egress speed limit, modifies the configuration of the speed limit uplink interface, and the distributed egress speed limit ACL resources will be updated to the newly configured uplink interface; Delete the configuration of the speed limit uplink interface, and the distributed egress speed limit ACL resources will be deleted;

For devices that support egress speed limit, modifying and deleting the configuration of the uplink interface will not affect the egress speed limit ACL resources.

By default, the user speed limit uplink port is not configured.

Table 1170 Configure the uplink port of the user speed limit

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the uplink port of the user speed limit	dot1x rate-limit uplink { interface *interface-name* | link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the uplink port of the user speed limit in the port.

Configure the Uplink Port of User Speed Limit

In the scenario where the user-based egress speed limit is distributed through the server, if the device does not support egress ACL, we need to configure this function. If the device supports the egress ACL, this configuration is ignored, and we do not need to configure this function.

When the device does not support the egress ACL, the user authenticates successfully and distributes the egress speed limit, modifies the configuration of the speed limit uplink interface, and the distributed egress speed limit ACL resources will be updated to the newly configured uplink interface; Delete the configuration of the speed limit uplink interface, and the distributed egress speed limit ACL resources will be deleted;

For devices that support egress speed limit, modifying and deleting the configuration of the uplink interface will not affect the egress speed limit ACL resources.

By default, the user speed limit uplink port is not configured.

Table 1171 Configure the uplink port of the user speed limit

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
Configure the uplink port of the user speed limit	dot1x rate-limit uplink { interface *interface-name* | link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the uplink port of the user speed limit in the port.

9.12.2.6 802.1X Monitoring and Maintaining

Table 1172 802.1X monitoring and maintaining

Command	Description
clear dot1x statistic [interface *interface-name* | interface 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 authentication user [interface *interface-name* | interface link-aggregation *link-aggregation-id* | mac *mac-address* | summary]	Display the authentication management user information
show authentication intf-status [interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Display the authentication status 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 auth-address [*mac-address* | interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Display the authenticable host list information
show dot1x config [interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Display the authentication configuration information
show dot1x free-ip	Display the secure channel configuration information
show dot1x global config	Display the global configuration information
show dot1x statistic [interface *interface-name* |	Display the authentication statistics information

Command	Description
interface link-aggregation *link-aggregation-id* | mac { *mac-address* | all }]	
show dot1x user [interface *interface-name* | interface link-aggregation *link-aggregation-id* | summary]	Display the user information

9.12.3 802.1X Typical Configuration Example

9.12.3.1 Configure 802.1X Portbased Authentication

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

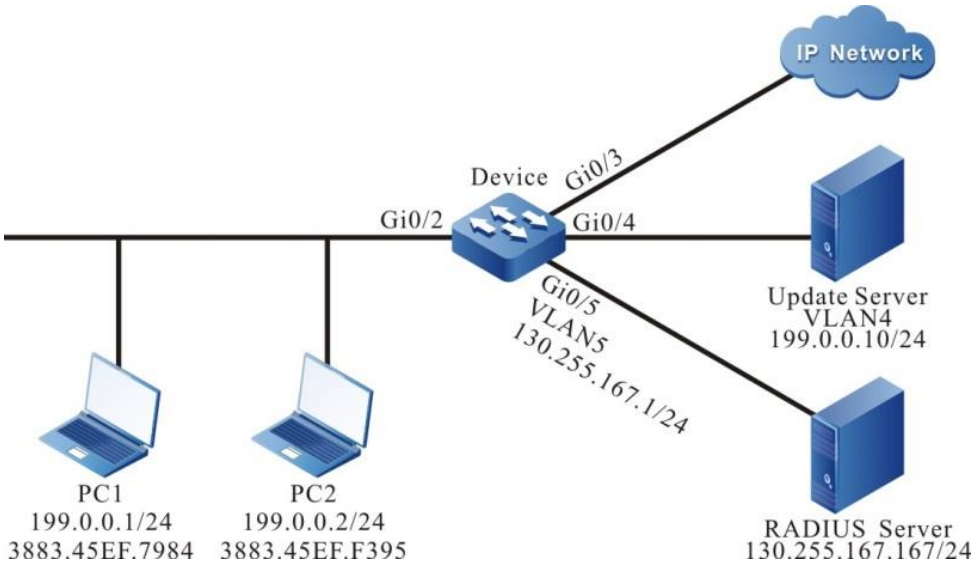


Figure 250 Networking of configuring 802.1X Portbased authentication

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)#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 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)# authentication 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)# authentication 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          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 hours 0 minute 51 seconds

Total: 1    Authorized: 1   Unauthorized/guest/critical: 0/0/0   Unknown: 0
```

9.12.3.2 Configure 802.1X Macbased Authentication

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, only 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

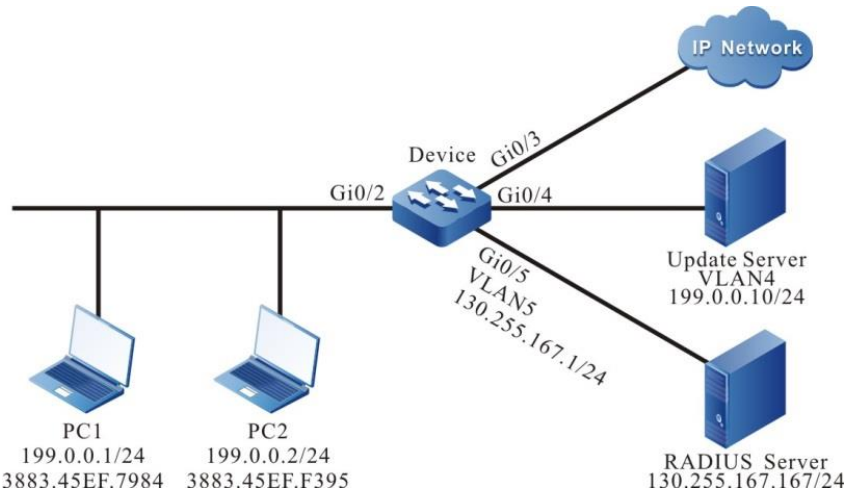


Figure 251 Networking of configuring 802.1X Macbased authentication

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)#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 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)#authentication 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)# authentication 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 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          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 hours 0 minute 51 seconds

 Total: 1    Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0   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.f395  STATUS=    Unauth(guest)    USER_NAME=  admin
      VLAN=      4          INTERFACE=  gi0/2        USER_TYPE=  DOT1X
      AUTH_STATE=  GUEST_HELD    BACK_STATE=  IDLE         IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown

 Total:1    Authorized: 0   Unauthorized/guest/critical: 0/1/0   Unknown: 0
```

9.12.3.3 Configure 802.1X Transparent Transmission Mode

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

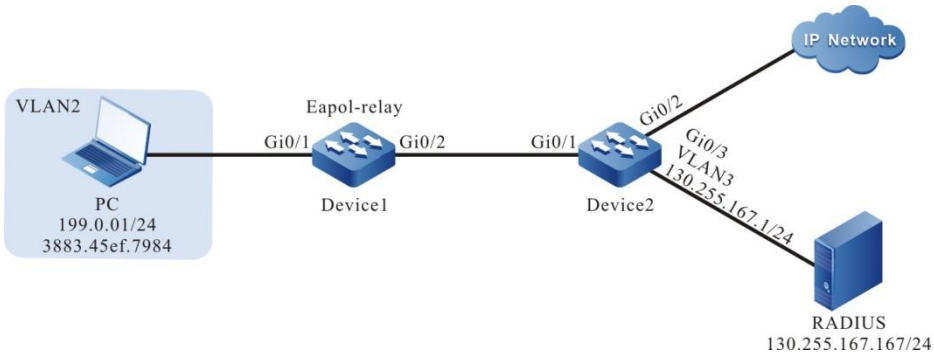


Figure 252 Networking of configuring the 802.1X transparent transmission mode

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.

```
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 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)# authentication 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=  2  INTERFACE=  gi0/1  USER_TYPE=  DOT1X
     AUTH_STATE=  AUTHENTICATED  BACK_STATE=  IDLE  IP_ADDRESS=  Unknown
     IPV6_ADDRESS= Unknown

     Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1  Authorized: 1 GetIP: 0  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

9.12.3.4 Configure 802.1X Free-Client Authentication

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

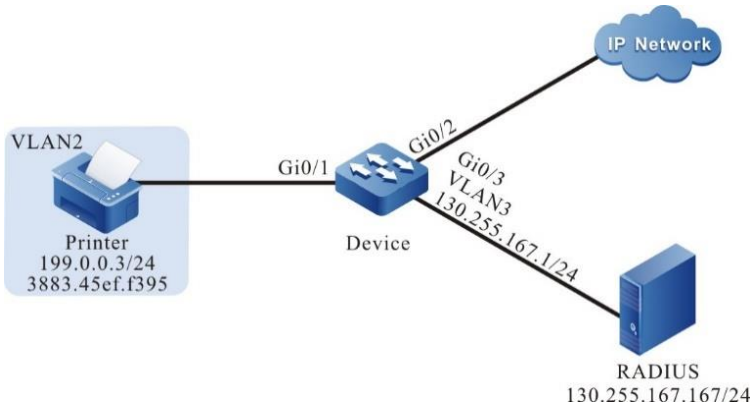


Figure 253 Networking of configuring the 802.1X free-client authentication

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)#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 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  INTERFACE= gi0/1  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 1 minutes 6 seconds
Total: 1 Authorized: 1 GetIP: 0 Unauthorized/guest/critical: 0/0/0 Unknown: 0

9.12.3.5 Configure Secure Channel

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

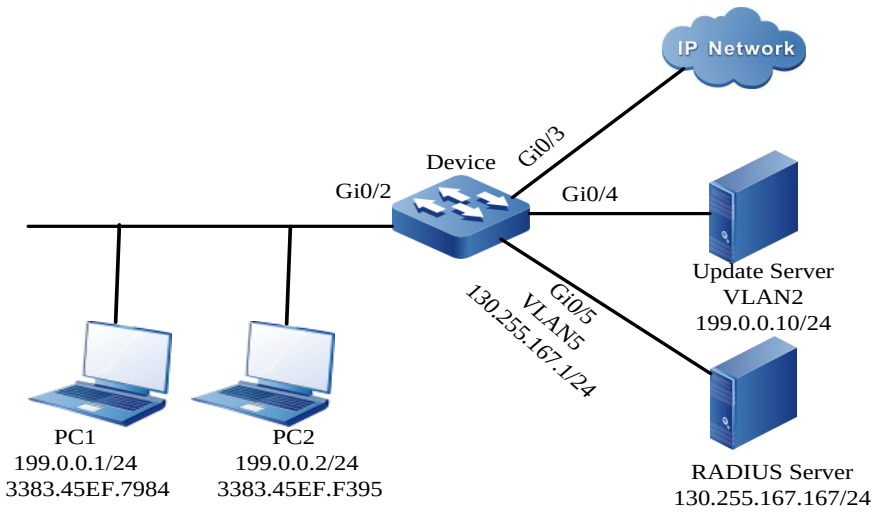


Figure 254 Networking of configuring secure channel

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(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 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 configure 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 enabled on the interface gigabitethernet 0/2 and the interface is bound to the channel secure channel rule.

#PC1 can visit 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          INTERFACE=  gi0/2       USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED  BACK_STATE= IDLE        IP_ADDRESS= 199.0.0.1
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 0 minute 51 seconds

 Total: 1   Authorized: 1 GetIP: 0  Unauthorized/guest/critical: 0/0/0   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.

9.12.3.6 Configure IP Authorization DHCP Server Mode

Network Requirements

- PC is connected to IP Network via Device; Device enables the 802.1X access control;
- Authentication mode adopts RADIUS authentication.
- PC1 gets the IP address via the specified DHCP server, and then can access IP Network.
- After being configured to carry the static IP address authentication, PC2 cannot access IP Network.

Network Topology

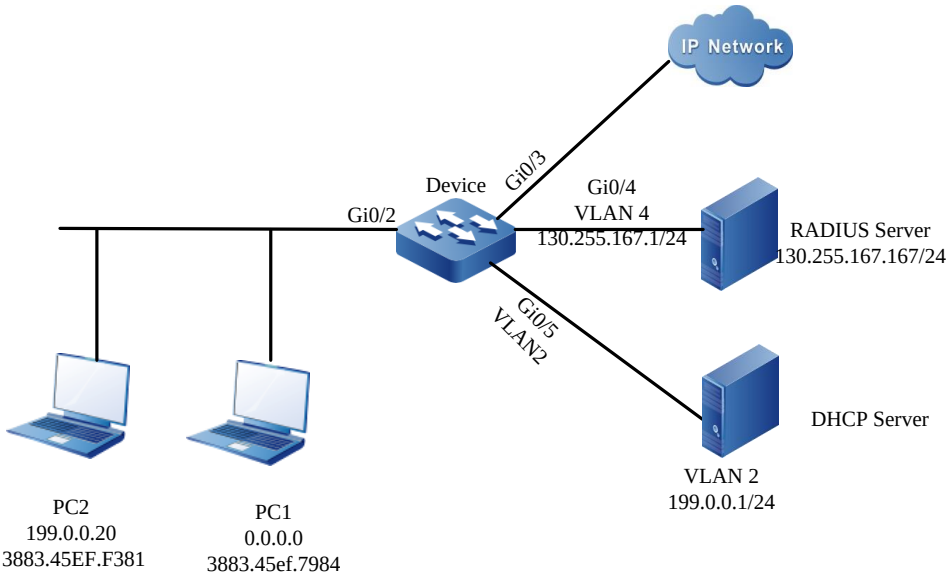


Figure 255 Networking of configuring 802.1X IP authorization DHCP Server mode

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on Device.

#Create VLAN2 and VLAN4 on Device, configure the port link type as Hybrid on gigabitethernet0/2, permit the services of VLAN2 to pass and configure PVID as 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 gigabitethernet0/5 of Device, configure the port link type as Access, permit the services of VLAN2 to pass (omitted).

#Configure the port link type as Access on gigabitethernet0/4 of Device, permit the services of VLAN4 to pass (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN4 as 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 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)#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 the AAA server.

#On the AAA server, configure the user name and password and key value as admin (omitted).

Step 5: Configure the DHCP server.

#On the DHCP server, configure the distributed IP address segment as 199.0.0.2-199.0.0.10 and the subnet mask as 255.255.255.0 (omitted).

Step 6: Enable the DHCP Snooping function on Device and configure the port gigabitethernet0/5 of Device as trust 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: Configure the 802.1X authentication on Device.

#Enable the 802.1X authentication of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the IP authorization of gigabitethernet0/2 as DHCP server mode.

```
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 the ARP keepalive of gigabitethernet0/2.

```
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.

#PC1 user can authenticate successfully and can get the IP address from the DHCP server and 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 GetIP: 0  Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#After PC2 user authenticates, it is in the GET-IP state and cannot get the 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  GetIP: 0 Unauthorized/guest/critical: 1/0/0 Unknown: 0
```

#After checking, PC2 cannot access IP Network.

9.12.3.7 Configure 802.1X Critical VLAN

Network Requirements

- PC is connected to IP Network via Device; Device enables the 802.1X access control;
- Authentication mode adopts RADIUS authentication.
- When PC fails to authenticate because the server is not available, only permit accessing Update Server.

Network Topology

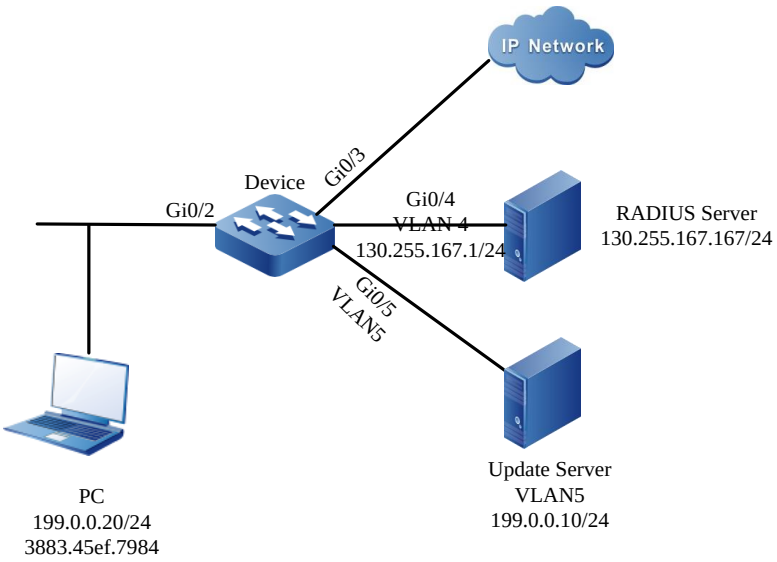


Figure 256 Networking of configuring 802.1X Critical VLAN

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on Device.

#Create VLAN2, VLAN4, and VLAN5 on Device, configure the port link type as Hybrid on gigabitethernet0/2, permit the services of VLAN2 to pass and configure

PVID as 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 gigabitethernet0/5 of Device, configure the port link type as Access, permit the services of VLAN5 to pass (omitted).

#Configure the port link type as Access on gigabitethernet0/4 of Device, permit the services of VLAN4 to pass (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN4 as 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 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)#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 the AAA server.

#On the AAA server, configure the user name and password and key value as admin (omitted).

Step 5: Configure the 802.1X authentication on Device.

#Enable the 802.1X authentication of gigabitethernet 0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#Enable MAC VLAN of gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)exit
```

#Configure Critical VLAN of the port as 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.

#Because the server is abnormal, Device cannot ping the server. As a result, the user authentication fails because the server is not available. PC user is in Critical VLAN and can access Update Server.

```
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 GetIP: 0  Unauthorized/guest/critical: 0/0/1 Unknown: 0
```

#The 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
```

9.12.3.8 Configure Using 802.1x with Port Security

Network Requirements

- PC is connected to IP Network via Device; Device enables the 802.1X access control and port security;
- Authentication mode adopts RADIUS authentication.
- Configure the port security rule of not matching the MAC address of PC1, and PC1 can pass the authentication and access IP Network.
- Configure the port security deny rule of matching the MAC address of PC2, and PC2 cannot pass the authentication.

Network Topology

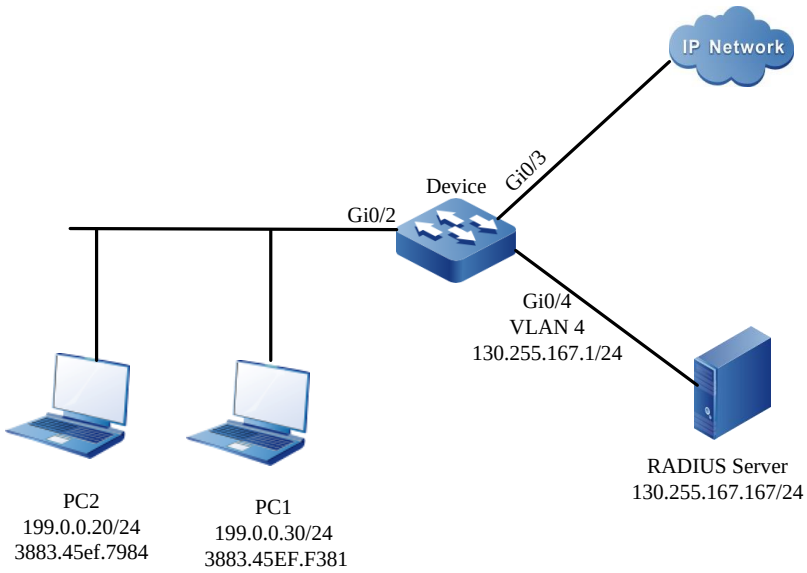


Figure 257 Networking of configuring using 802.1X with port security

Configuration Steps

Step 1: Configure the link type of the VLAN and interface on

Device.

#Create VLAN2, VLAN4, and VLAN5 on Device, configure the port link type as Hybrid on gigabitethernet0/2, permit the services of VLAN2 to pass and configure PVID as 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 gigabitethernet0/4 of Device, configure the port link type as Access, permit the services of VLAN4 to pass (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN4 as 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 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)#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 the AAA server.

#On the AAA server, configure the user name and password and key value as admin (omitted).

Step 5: Configure the 802.1X authentication on Device.

#Enable the 802.1X authentication on gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure the port security on Device.

#Enable the port security on the port gigabitethernet0/2.

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)exit
```

#Configure the port security rule on the port gigabitethernet0/2.

```
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 authenticate successfully and access IP Network after passing the 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 GetIP: 0  Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

#PC2 user cannot authenticate successfully and cannot access the network.

9.13 PORTAL

9.13.1 Overview

9.13.1.1 Portal Overview

Portal authentication is also known as Web authentication, that is, authenticate the user by accepting the user name and password entered by the user through the Web page. The Portal authentication technology provides a flexible access control method. Without installing the client, access control can be implemented at the access layer and the key data entry that needs to be protected. Portal authentication website is generally called portal website.

When unauthenticated users access the network, the device forces users to access a specific site, that is, the Portal server. Without authentication, users can access the services free of charge, such as application program (such as anti-virus software and operating system patches) upgrade. When users need to use other resources in the Internet, they must authenticate their identity on the Portal authentication page provided by the Portal server. They can use the network resources only after passing the authentication.

In addition to the flexibility of authentication, Portal can also provide convenient management functions. On the Portal authentication page, you can carry out personalized services such as advertising and notification.

9.13.1.2 Portal System Composition

The typical networking method of Portal is shown in the following figure. It consists of four elements: Portal Client, Authentication Device, Portal Server (Portal server) ,and AAA Server (authentication/authorization/statistics server, referred to as AAA server).

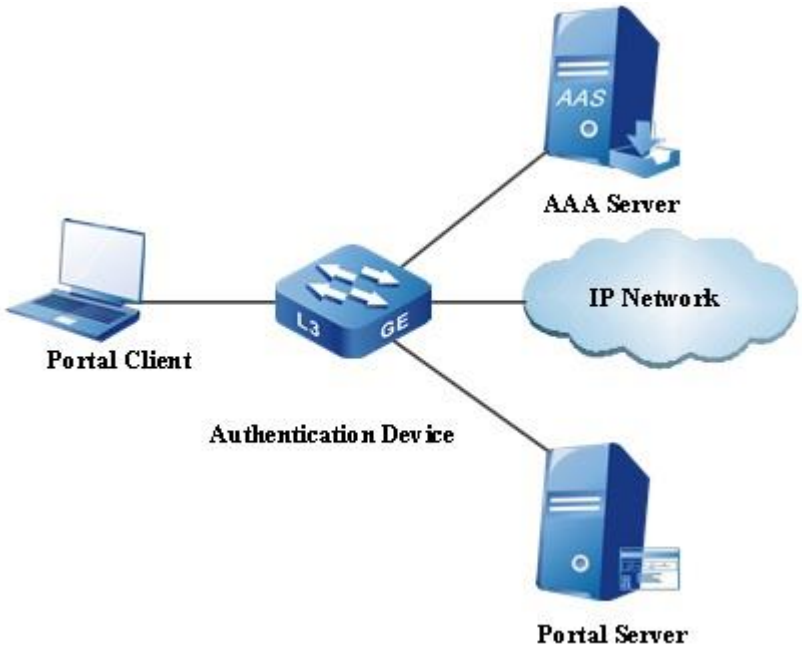


Figure 258 Portal system composition

- Authenticated Client: Usually, it is the browser running the HTTP protocol, and also can be the proprietary Portal client software.
- Authentication device: The authentication device is located between the client and the authentication server. It controls the network access of the client by interacting with the Portal server and AAA server.
- Portal Server: The server-side system that receives authentication requests from authentication clients, provides free portal services and Web-based authentication interface. Portal Server accepts authentication requests from authentication clients, extracts the authentication information, interacts with authentication devices through the Portal protocol, and notifies the authentication clients of authentication results.
- AAA Server: Usually, it is the RADIUS (Remote Authentication Dial-In User Service) server, used to verify the validity of the client and notify the authentication result to the authentication device. The authentication device controls the network access of the client according to the authentication result.

9.13.1.3 Portal Authentication Modes

In different networking modes, the available Portal authentication modes are different, distinguished by the network layers that implements the Portal authentication in the network. The Portal authentication modes are divided to two kinds: L2 authentication mode and L3 authentication mode.

1. L2 authentication mode

Support enabling the Portal authentication function on the L2 interface of the authentication device connecting the user. Users can only access the Portal server by manually configuring or DHCP to directly get an IP address before authentication; after authentication, they can access network resources. The L2 authentication mode is based on the source MAC control, which allows the packets with the valid source MAC address to pass after passing the authentication.

2. L3 authentication mode

Support enabling the Portal authentication function on the L3 interface of the authentication device connecting the user. The L3 authentication mode can be divided into ordinary L3 authentication mode and secondary address assignment authentication mode.

1) Ordinary L3 authentication mode

Users can only access the Portal server and the set free access address by manually configuring or DHCP to directly get an IP address before authentication; after authentication, they can access network resources. The ordinary L3 authentication mode has two control modes:

- Control based on source IP: Permit the packet with the valid source IP to pass after passing the authentication
- Control based on source IP + source MAC: Permit the packet with the valid source IP and source MAC to pass after passing the authentication

9.13.1.4 Portal Authentication Process

There are two authentication interaction modes between the Portal server and authentication device:

- CHAP (Challenge Handshake Authentication Protocol) authentication interaction: The user name and password are encrypted to transmit, with high security
- PAP (Password Authentication Protocol) authentication interaction: The user name and password are transmitted with plain text, with low security

To adopt the CHAP authentication interaction, the Portal server will perform inquiry handshake verification. Challenge is generated at random when the authentication device receives the request Challenge packet, the length is 16 bytes, and it is delivered to the Portal server with the Challenge response packet.

The L2 Portal authentication process is the same as the ordinary L3 Portal authentication process.

1. The flow of L2 Portal authentication and ordinary L3 Portal authentication

The flowchart is as follows:

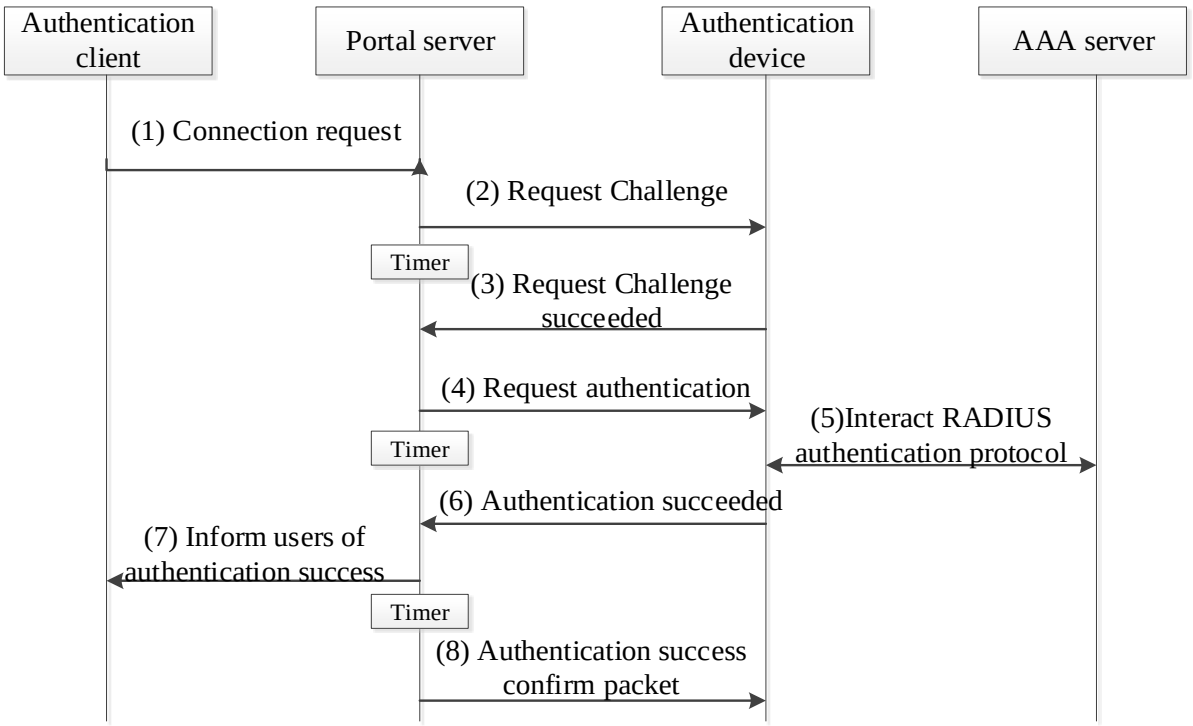


Figure 259 CHAP flowchart of L2/ordinary L3 Portal authentication

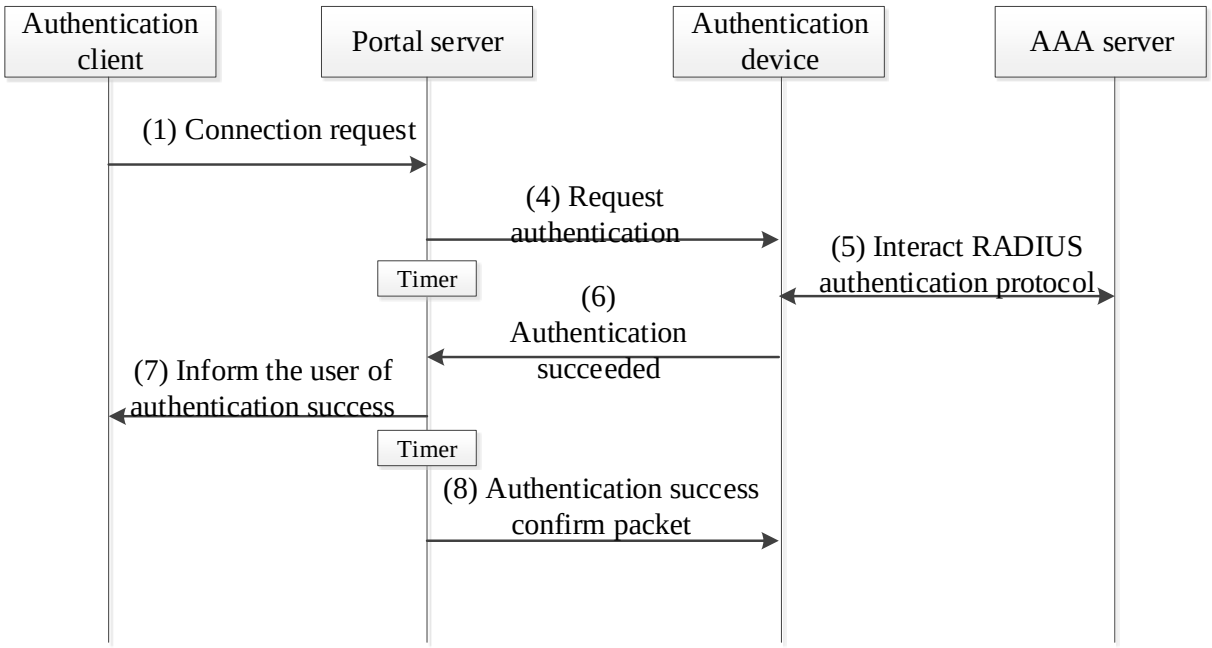


Figure 260 The PAP flowchart of L2/ordinary L3 Portal authentication

The flow of the L2 Portal authentication and ordinary L3 Portal authentication:

1. Portal users initiate authentication requests through the HTTP protocol when they need to access the network. When the HTTP packet passes the authentication device, the authenticated device allows the HTTP packet accessing the Portal server or with the set free access address to pass; for the HTTP packet accessing other addresses, the authentication device intercepts and redirects it to the Portal server. The Portal server provides the Web page for users to enter the valid usernames and passwords registered on the authentication server to start an authentication process.
2. The Portal server adopts the CHAP authentication interaction to verify the inquiry handshake, and the Portal server requests Challenge from the authentication device. Adopt the PAP authentication interaction to directly perform step (4).
3. The authentication device randomly generates Challenge when receiving the request Challenge packet, sends the request Challenge success packet, and delivers Challenge to the Portal server. Adopt the PAP authentication

interaction to directly perform step (4).

4. The Portal server assembles the user name and password input by the user into a request authentication packet and sends it to the authentication device to request authentication. At the same time, enable the timer to wait for the authentication response.
5. Interact the RADIUS protocol packet between the authentication device and RADIUS server.
6. The authentication device sends the authentication success packet to the Portal server.
7. The Portal server sends the authentication pass packet to the authentication client, informing the user of the authentication success.
8. The Portal server sends the authentication success confirm packet to the authentication device.

9.13.1.5 Support Delivering ACL

ACL (Access Control List) provides the function of controlling the user accessing network resources and restricting users' access authority. When the user is online, and if the authorized ACL is configured on the server, the device will control the data flow of the user's port according to the authorized ACL issued by the server. Before configuring the authorized ACL on the server, it is necessary to configure the corresponding rules on the device. L2 Portal authentication supports delivering the IP standard ACL and IP extended ACL, and L3 Portal authentication supports delivering the IP extended ACL, but the matching items of the configured ACL rules support adding “source IP + source MAC”.

9.13.2 Portal Function Configuration

Table 1173 Portal function configuration list

Configuration Task	
Configure the Portal server and attributes	Create a Portal server
	Configure the Portal server type
	Configure the Portal server detection

Configuration Task	
	function
	Configure the source interface used by sending the Portal packet
	Configure the destination UDP port number of sending the user forced offline packet
Configure the L2 Portal authentication function	Enable the L2 Portal authentication function
Configure the L2 Portal authentication attributes	Configure the port access control mode
Configure the L3 Portal authentication function	Enable the ordinary L3 Portal authentication function
	Configure and apply secure channel
Configure the public attributes	Configure the maximum users of the interface
	Configure the user authentication migration function
	Configure whether to carry the domain name
	Configure the timer parameters
	Configure the authentication method list
	Configure the statistics method list

9.13.2.1 Configure the Portal Server and Attributes

Configuration Condition

None

Create a Portal Server

Create a Portal server and specify the related parameters of the Portal server, including the IP address of the server, shared encrypted key, server port number, and server URL (the authentication page address of the server).

Table 1174 Create a Portal server

Step	Command	Description
Enter global configuration	configure terminal	-

Step	Command	Description
mode		
Create a Portal server	portal server *server-name* ip *ip-address* key [0 | 7] *key-string* [port *udp-port-num* | url *url-string*]	Optional By default, do not create a Portal server.

Note

- The Portal protocol only supports the IPv4 protocol.
- Up to 5 Portal servers are created on the authentication device.
- The configured Portal server parameters can be deleted or modified only when the Portal server is not referenced by the interface.
- The configured share keys on the authentication device and Portal server should be consistent.

Configure the Portal Server Type

Configuring the Portal server type has two aspects of functions:

- Different Portal servers do some expansions the standard Portal protocol specifications.
- When the Portal server is not configured with the server URL, the Portal server uses the default server URL of the corresponding type to re-direct.

The following server types can be specified:

aas: The AAS server, default server URL: http://IP-ADDRESS/portal/Login.do

imc: The IMC server, default server URL: http://IP-ADDRESS:8080/porta

user-defined: User-defined server. The default server URL format follows the protocol specification <PORTAL protocol specification for China Mobile WLAN service v2.0.2>.

Table 1175 Configure the Portal server type

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the Portal server type	portal server *server-name* type { aas | imc | user-defined }	Optional By default, the server type is AAS.

Configure Portal Server Detection Function

In the process of the Portal authentication, if the communication between the authentication device and the Portal server is interrupted, the new users cannot be able to get online, and the existing online Portal users cannot be able to get offline normally. To solve these problems, it is necessary that the authentication device can detect the change of the reachable state of the Portal server in time, and trigger the corresponding operations to deal with the impact of the change. For example, when a specified Portal server is not reachable, all users who authenticate using the Portal server will be forced to pass the authentication, so as to access network resources, which is commonly referred to as the Portal escape function.

With the detection function, the authentication device can detect the reachable status of the Portal server. The specific configuration is as follows:

1. The interval of detecting whether the server is reachable
2. The action when the reachable status of the server changes

- Record the log: Record the log information when the reachable status of the Portal server changes
- Open user limitation: When the reachable status of the Portal server change, record the log information. When the specified Portal server is unreachable, all users who use the Portal server to authenticate are forced to pass the authentication. When the Portal server is reachable again, force the user who is forced to pass authentication using the Portal server to get offline.

Table 1176 Configure the Portal server detection function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the interval of detecting the Portal server	portal server *server-name* detect-interval *detect-interval-value*	Optional By default, the interval of detecting the Portal server is 60s, and the value range is 20-600s or 0. When it is configured as 0, do not detect the Portal server.
Configure the action when the reachable status of the Portal server changes	portal server *server-name* failover { log | permit }	Optional By default, record the log information when the reachable status of the Portal server changes.

Configure the Source Interface Used by Sending the Portal Packet

Specify the source interface used by sending the Portal packet. The configured master IP address in the source interface is the source address used by the authentication device to send the Portal packet to the Portal server. If there is no master IP address in the source interface, the communication will fail.

Table 1177 Configure the source interface used by sending the Portal packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the source interface used by sending the Portal packet	portal server *server-name* source-interface *interface-name*	Optional By default, do not specify the source interface used by sending the Portal packet, that is, take the interface of

Step	Command	Description
		connecting the user as the source interface of sending the Portal packet.

Configure the Destination UDP Port Number of User Forced Offline Packet

The port number of some server for receiving the user forced offline packet is the specified UDP port number, so it is necessary to configure the destination UDP port number of the user forced offline packet.

Table 1178 Configure the destination UDP port number of the user forced offline packet

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the destination UDP port number of the user forced offline packet	portal server *server-name* ntf-logout-port *udp-port-num*	Optional By default, do not specify the destination UDP port number of the user forced offline packet, but adopt the server port number as the destination UDP port number of the user forced offline packet.

9.13.2.2 Configure the L2 Portal Authentication Function

Configuration Condition

To enable the L2 Portal authentication function, it is necessary to meet the following conditions:

- The Portal server is created on the authentication device

Enable L2 Portal Authentication Function

Enable the L2 Portal authentication on the port of connecting the user on the

authentication device. The L2 Portal authentication controls based on the source MAC, permitting the authenticated packet with the valid source MAC address to pass.

Table 1179 Enable the L2 Portal 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 interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enable the L2 Portal authentication function	portal server *server-name* method layer2	Mandatory By default, the L2 Portal authentication function of the port is disabled.

Note

- The L2 Portal authentication mode does not support VLAN delivery.
- On one port, you cannot configure the L2 Portal authentication or 802.1X Free-IP function at the same time.
- When the L2 Portal authentication is enabled on one port, the corresponding VLAN interface cannot enable the L3 Portal authentication. Otherwise, the configuration fails.
- When the port enabled with the L2 Portal authentication is added to the VLAN interface enabled with the L3 Portal authentication, clear the L2 Portal authentication configuration of the port automatically, and record

the log of auto clearing the configuration at the same time.

9.13.2.3 Configure L2 Portal Authentication Attributes

Configuration Condition

None

Configure Port Access Control Mode

There are two port access control modes: Port-based access control mode and user-based access control mode.

Port-based access control mode (Portbased): Only permit one user to pass the authentication in the port

User-based access control mode (Macbased): In the port permit multiple users to pass the authentication; the users in the port can access the network only after passing the authentication.

Port-based access control mode is divided to two types: 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, and the other users cannot access the network and cannot pass the authentication.

Table 1180 Configure the 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,
Enter the aggregation group	interface link-aggregation *link-*	

Step	Command	Description
configuration mode	*aggregation-id*	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.
Configure the access control mode	authentication port-method { macbased | portbased }	Mandatory By default, enable the user authentication mode in the port.
Port-based access control mode	authentication 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 in the port-based access control mode, it is necessary to ensure that the access control mode has been configured as port-based access control mode (Portbased).

9.13.2.4 Configure L3 Portal Authentication Function

Configuration Condition

To enable the L3 Portal authentication function, it is necessary to meet the following condition:

- The Portal server is created on the authentication device

Enable Ordinary L3 Portal Authentication Function

On the L3 interface of the authentication device connecting the user, enable the

ordinary L3 Portal authentication function. The ordinary L3 authentication mode has two control modes:

- Control based on the source IP: Permit the authenticated packet with the valid source IP to pass
- Control based on the source IP + source MAC: Permit the authenticated packet with the valid source IP and source MAC address to pass

Table 1181 Enable the ordinary L3 Portal authentication function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the ordinary L3 Portal authentication function	portal server *server-name* method layer3 [ip | ip-mac]	Mandatory By default, the ordinary L3 Portal authentication function is disabled.

Note

- You cannot enable the 802.1X authentication and MAC authentication function on the port that is enabled with the ordinary L3 Portal authentication.
- You cannot enable the L2 Portal authentication function on the port that is enabled with the ordinary L3 Portal authentication.
- When the port enabled with the L2 Portal authentication is added to the VLAN interface enabled with the ordinary L3 Portal authentication, the L2 Portal authentication will be disabled.

Enable the Portal Authentication Function of Secondary Address Assignment

Enable the Portal authentication function of the secondary address assignment on the L3 interface of the authentication user connecting the user. The Portal authentication function of the secondary address assignment controls based on the source IP + source MAC, permitting the authenticated packet with the valid source IP and source MAC address to pass.

To configure the Portal authentication function of secondary address assignment, it is necessary to meet the following conditions:

- Configure the active and standby IP addresses on the interface
- The DHCP Relay and DHCP Snooping functions need to be configured on the authentication device.

Table 1182 Enable the Portal authentication function of the secondary address assignment

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the Portal authentication function of the secondary address assignment	portal server *server-name* method redhcp	Mandatory By default, the Portal authentication function of the secondary address assignment is disabled on the interface.

Note

- You cannot enable the 802.1X authentication and MAC authentication function on the port that is enabled with the Portal authentication interface of the secondary address assignment.
- You cannot enable the L2 Portal authentication function on the port that is enabled with the Portal authentication interface of the secondary address assignment.

- When the port enabled with the L2 Portal authentication is added to the VLAN interface enabled with the Portal authentication of the secondary address assignment, the L2 Portal authentication will be disabled.
- The Portal authentication mode of the secondary address assignment needs to be supported by the Portal client and Portal server at the same time. Otherwise, the authentication cannot be done.

Configure and Apply Secure Channel

After enabling the L3 authentication function on the L3 interface, it is necessary to configure and apply the secure channel if hoping to allow the terminal users to access the resources in the specified network without authentication or to specify the specific terminal users to access the network resources without authentication.

Configuring the secure channel rules can be divided to the following types:

- Configure the terminal user to permit accessing the specified network resources
- Configure the specified terminal user to permit accessing network resources

Table 1183 Apply the secure channel

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the secure channel	hybrid access-list advanced { *access-list-number* | *access-list-name* }	Mandatory By default, the secure channel is not configured in the device.
Configure the secure channel rules	[*sequence*] permit *protocol* { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any | *source-mac-addr source-wildcard* | host *source-mac-addr* } { any | *destination-*	Mandatory By default, there is no secure channel rule in the secure channel.

Step	Command	Description
	ip-addr destination-wildcard | host *destination-ip-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* }	
Apply the secure channel	global security access-group { *access-group-number* | *access-group-name* }	Mandatory By default, do not apply any secure channel in the system.

Note

- The device can configure multiple secure channels, and one secure channel can be configured with multiple secure channel rules.
- The secure channel type can only be the mixed advanced ACL. In the device, only permit applying one secure channel.

9.13.2.5 Configure Public Attributes

Configuration Condition

None

Configure Max. Users of the Interface

If the authenticated users in the interface reach the configured threshold, the authentication system does not respond to the authentication requests of the new users. The value range of the maximum users of the L2 interface is 1-4096. The value range of the maximum users of the L3 interface is 1-500.

Table 1184 Configure the maximum users of the interface

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 interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group. After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the interface configuration mode	interface *interface-name*	
Configure the maximum users of the interface	authentication max-user-num *max-user-num-value*	Mandatory By default, the maximum number of the users permitted to be connected in the interface is 256.

Note

- In the L2 interface, it is necessary to configure as the user-based access control mode (Macbased). Otherwise, the configured number of the users that are permitted to be connected does not take effect.

Configure User Authentication Transfer Function

The user authentication transferring function applies to the scenario where the same user transfers from one authentication port of the same device to another. When the user authentication transferring function is disabled, the user is not allowed to

initiate authentication on another authentication port of the device after being authenticated on one port of the device; when the user authentication transferring function is enabled, and after the user is authenticated on one port, the device first deletes the authentication information on the original port after detecting that the user transfers to another authentication port, and then, allows the user to initiate authentication on the new authentication port

Whether or not user authentication transferring function is enabled, the device will record the log when detecting that the user transfers between the authentication ports.

Table 1185 Configure the user authentication transferring 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 configuration just takes effect on the aggregation group. After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the interface configuration mode	interface *interface-name*	
Configure the user authentication migration function	authentication station-move { enable | disable }	Mandatory By default, the user authentication migration function is disabled.

Configure Whether to Carry Domain Name

In some scenarios, when the client initiates authentication, the user name will automatically carry the domain name, and the user carrying the domain name will fail to authenticate on the authentication server. To avoid this case, the authentication device can configure whether the authentication user name format sent to the authentication server carries the domain name.

Table 1186 Configure whether to carry the domain name

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 configuration just takes effect on the aggregation group. After entering the interface configuration mode, the subsequent configuration just takes effect on the current interface.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the interface configuration mode	interface *interface-name*	
Configure whether to carry the domain name	portal user-name-format { with-domain | without-domain }	Mandatory By default, carry the domain name.

Configure Timer Parameters

In the interface the timer parameters contain authenticating timeout timer, authenticated timeout timer, idle detection timer, and quiet timer.

Authenticating timeout timer (authenticating-period): When detecting that there is the client packet, enable the authenticating timeout timer. After the timer times out and if there is no authentication result, the client is deleted.

Authenticated timeout timer (authenticated-period): When the client is authenticated successfully, enable the authenticated timeout timer. After the timer times out, force to delete the authenticated client information.

Idle detection timer (idle-period): When the client is authenticated successfully, enable the idle detection timer. After detecting that the client is offline, force to delete the authenticated client information.

Quiet timer (quiet-period): After the client failed to be authenticated, enable the quiet timer. After the quiet timer times out, the authentication device responds to the client authentication request again.

The new times can only be valid for the subsequent online authentication user, not valid for the online authentication user.

Table 1187 Configure the 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 interface. After entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group. After entering the interface configuration mode, the subsequent configuration just takes effect on the current
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	
Enter the interface configuration mode	interface *interface-name*	

Step	Command	Description
		interface.
Configure the timer parameters	portal timeout { authenticating-period *authenticating-period-value* | authenticated-period *authenticated-period-value* | idle-period *idle-period-value* | quiet-period *quiet-period-value* }	Mandatory By default, the time of the authenticating timeout timer is 120s, and the value range is 15-300; the time of the authenticated timeout timer is 3600s, and the value range is 300-864000; the time of the idle detection timer is 300s, 0 or 180-1800; the quiet time is 60, and the value range is 15-3600.

Configure Authentication Method List

Configure the authentication method list used by the Portal user. When the user name of the Portal user carries the domain name, use the authentication method list specified by the domain name. When the user name of the Portal user does not carry the domain name, use the configured authentication method list.

Table 1188 Configure the authentication method list

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the connection authentication method list	portal authentication method-list { default | *list-name* }	Optional By default, use the default authentication method list.

Configure Statistics Method List

Configure the statistics method list used by the Portal user. When the user name of the Portal user carries the domain name, use the statistics method list specified by the domain name; when the user name of the Portal user does not carry the domain

name, use the configured statistics method list.

Table 1189 Configure the statistics method list

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the connection statistics method list	portal accounting method-list { default | *list-name* }	Optional By default, use the default statistics method list.

9.13.2.6 Portal Monitoring and Maintaining

Table 1190 Portal monitoring and maintaining

Command	Description
clear portal user { ip *ip-address* | mac *mac-address* | all | interface *interface-name* | link-aggregation *link-aggregation-id* }	Force the Portal user offline
clear portal auth-fail-user history [ip *ip-address*]	Clear the authentication failure record information
clear portal statistic [interface *interface-name* | link-aggregation *link-aggregation-id*]	Clear the authentication statistics information
show authentication user [ip *ip-address* | mac *mac-address* | all | interface *interface-name* | link-aggregation *link-aggregation-id* | summary]	Display the authentication management user information
show authentication intf-status [interface *interface-name* | link-aggregation *link-aggregation-id*]	Display the authentication status information
show portal	Display the authenticated default configuration information
show portal auth-fail-user history [ip *ip-address* | recent]	Display the authentication failure information
show portal config [interface *interface-name* | link-aggregation *link-aggregation-id*]	Display the authentication configuration information
show portal global config	Display the global configuration information

Command	Description
show portal server	Display the Portal server information
show portal statistic [interface *interface-name* | link-aggregation *link-aggregation-id*]	Display the authentication statistics information
show portal user [ip *ip-address* | mac *mac-address* | interface *interface-name* | link-aggregation *link-aggregation-id* | summary]	Display the user information

9.13.3 Portal Typical Configuration Example

9.13.3.1 Configure Portbased Authentication of L2 Portal Authentication

Network Requirements

- PC1 and PC2 on one LAN are connected to IP Network via Device, enable the L2 Portal authentication function on Device, and configure the authentication mode as Portabased.
- The authentication mode adopts the RADIUS authentication.
- The un-authenticated user can only access Portal Server, and the authenticated user can access IP Network.
- After one user on LAN passes the authentication, the other users on the LAN can access IP Network without authentication.

Network Topology

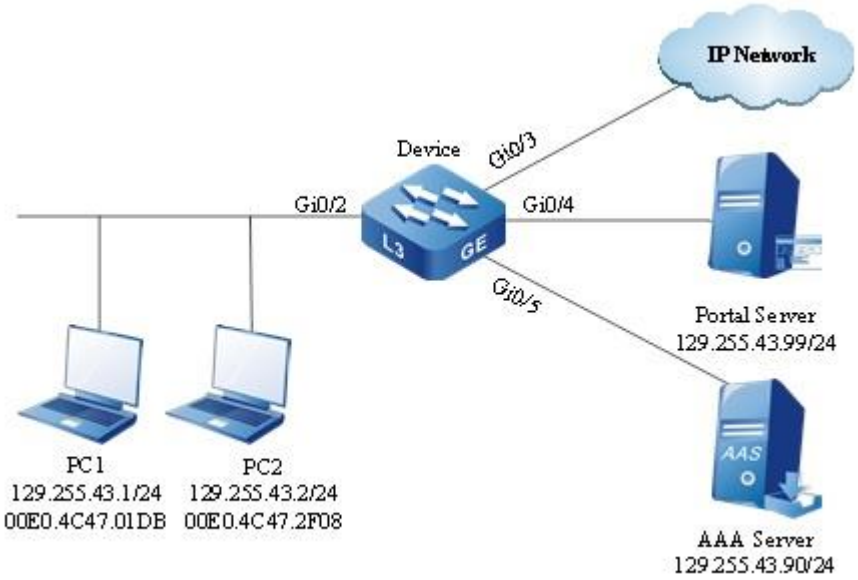


Figure 261 Networking of configuring the Portbased authentication of the L2 Portal authentication

Configuration Steps

Step 1: Configure the VLAN and port link type on Device.

#Create VLAN129 on Device.

```
Device#configure terminal
Device(config)#vlan 129
Device(config)#exit
```

#Configure the link type of port gigabitethernet0/2 as Access, permitting the services of VLAN129 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 129
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the port link type on gigabitethernet 0/3-gigabitethernet 0/5 of Device as Access, permitting the services of VLAN129 to pass (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device(config)#interface vlan 129
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
```

```
Device(config-if-vlan129)#exit
```

Step 3: Configure the AAA authentication.

#On Device, enable the AAA authentication, adopt the RADIUS authentication mode, the RADIUS server address is 129.255.43.90/24, the key value is admin, and the priority is 1.

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 129.255.43.90 priority 1 key admin
```

Step 4: Configure the AAA server.

#Configure the user name, password and key value as admin on the AAA server (omitted).

Step 5: Configure the L2 Portal authentication.

#On Device, configure the Portal server named server1.

```
Device(config)# portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
```

#On Device, enable L2 portal authentication, and the authentication mode is Portased.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#portal server server1 method layer2
Device(config-if-gigabitethernet0/2)#authentication port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure the Portal server.

#On the Portal server, configure the IP address, Device address and key of PC1 as admin (omitted).

Step 7: Check the result.

#Before passing the authentication, both PC1 and PC2 can only access Portal Server.

#PC1 can pass the authentication. Both PC1 and PC2 can access IP Network.

```
Device#show portal user
--------------------
NO 1  : IP_ADDRESS= 129.255.43.1  STATUS= Authorized   USER_NAME=  admin
      INTERFACE=  gi0/2       CTRL_METHOD= L2_MAC   AUTH_STATE=  AUTHENTICATED
      BACK_STATE= AAA_SM_IDLE   VLAN= 129         MAC_ADDRESS= 00E0.4C47.01DB

 Total: 1   Authorized: 1   Unauthorized/Guest/Critical: 0/0/0
```

9.13.3.2 Configure Macbased Authentication of L2 Portal Authentication

Network Requirements

- PC1 and PC2 on one LAN are connected to IP Network via Device, enable the L2 Portal authentication function on Device, and configure the authentication mode as Macbased.
- The authentication mode adopts the RADIUS authentication.
- The un-authenticated user can only access Portal Server, and the authenticated user can access IP Network.
- After one user on LAN passes the authentication, the user can access IP Network, and the other users on the LAN can access IP Network after passing the authentication.

Network Topology

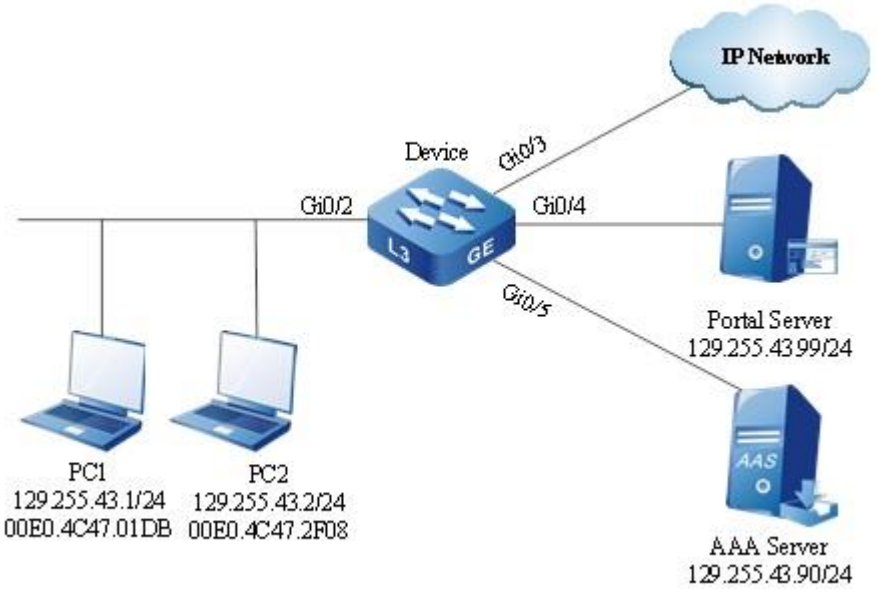


Figure 262 Networking of configuring the Macbased authentication of the L2 Portal authentication

Configuration Steps

Step 1: Configure the VLAN and port link type on Device.

#Create VLAN129 on Device.

```
Device#configure terminal
Device(config)#vlan 129
Device(config)#exit
```

#Configure the link type of port gigabitethernet0/2 as Access, permitting the services of VLAN129 to pass.

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 129
Device(config-if-gigabitethernet0/2)#exit
```

#Configure the port link type on gigabitethernet 0/3-gigabitethernet 0/5 of Device as Access, permitting the services of VLAN129 to pass (omitted).

Step 2: Configure the interface IP address of Device.

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device(config)#interface vlan 129
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
Device(config-if-vlan129)#exit
```

Step 3: Configure the AAA authentication.

#On Device, enable the AAA authentication, adopt the RADIUS authentication mode, the RADIUS server address is 129.255.43.90/24, the key value is admin, and the priority is 1.

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 129.255.43.90 priority 1 key admin
```

Step 4: Configure the AAA server.

#Configure the user name, password and key value as admin on the AAA server (omitted).

Step 5: Configure the L2 portal authentication.

#On Device, configure the Portal server named server1.

```
Device(config)# portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
#On Device, enable the L2 portal authentication, and the authentication mode is Macbased.
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#portal server server1 method layer2
Device(config-if-gigabitethernet0/2)#authentication port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

Step 6: Configure the Portal server.

#On the Portal server, configure the IP address, Device address and key of PC1 as admin (omitted).

Step 7: Check the result.

#Before passing the authentication, both PC1 and PC2 can only access Portal Server.

#PC1 can pass the authentication. PC1 can access IP Network, and PC2 cannot access IP Network.

```
Device#show portal user
--------------------
NO 1  : IP_ADDRESS= 129.255.43.1  STATUS= Authorized   USER_NAME=  admin
      INTERFACE=  gi0/2       CTRL_METHOD= L2_MAC  AUTH_STATE=  AUTHENTICATED
      BACK_STATE= AAA_SM_IDLE   VLAN= 129          MAC_ADDRESS= 00E0.4C47.01DB
 Total: 1   Authorized: 1   Unauthorized/Guest/Critical: 0/0/0
```

9.13.3.3 Configure Ordinary L3 Portal Authentication

Network Requirements

- PC1 and PC2 on one LAN are connected to IP Network via Device, and enable the ordinary L3 Portal authentication on Device.
- The authentication mode adopts the RADIUS authentication.
- Before passing the authentication, PC1 can only access Update Server. After passing the authentication, PC1 can access IP Network.
- PC2 can access Update Server.

Network Topology

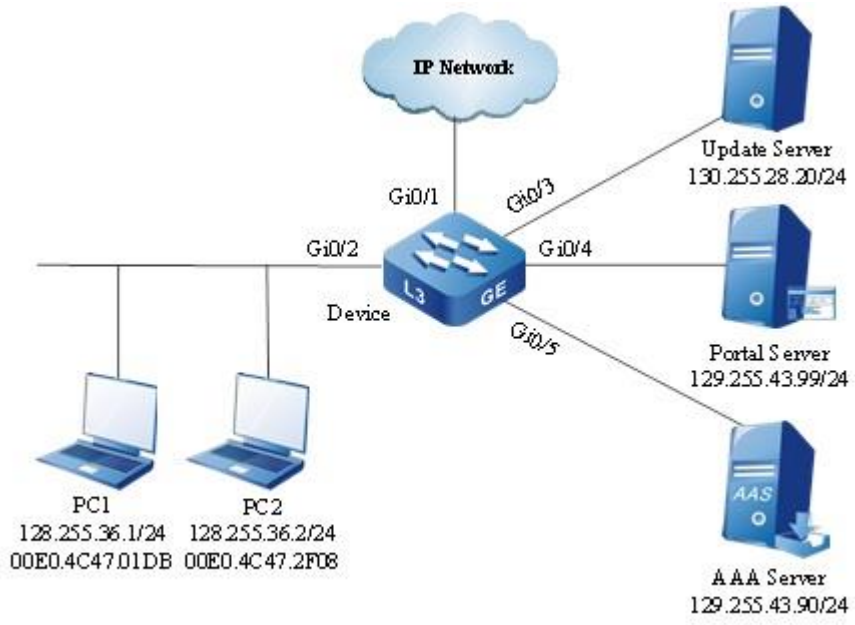


Figure 263 Networking of configuring the ordinary L3 Portal authentication

Configuration Steps

#On Device, create VLAN128, VLAN129, VLAN130, and VLAN131.

```
Device#configure terminal
Device(config)#vlan 128,129,130,131
Device(config)#exit
```

#Configutre the link type of port gigabitethernet0/2 as Access, permitting the services of VLAN128 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 128
Device(config-if-gigabitethernet0/2)#end
```

#Configutre the port link type on gigabitethernet0/1 of Device as Access, permitting the services of VLAN131 to pass. Configure the port link type on gigabitethernet0/3 of Device as Access, permitting the services of VLAN130 to pass. Configutre the port link type on gigabitethernet0/4-gigabitethernet 0/5 of Device as Access, permitting the services of VLAN129 to pass. (omitted)

Step 2: Configure the interface IP address of Device, ensuring that the

network route is reachable.

#Configure the IP address of VLAN128 as 128.255.36.10/24.

```
Device#configure terminal
Device(config)#interface vlan 128
Device(config-if-vlan128)#ip address 128.255.36.10 255.255.255.0
Device(config-if-vlan128)#end
```

#Configure the IP address of VLAN129 as 129.255.43.10/24.

```
Device#configure terminal
Device(config)#interface vlan 129
Device(config-if-vlan129)#ip address 129.255.43.10 255.255.255.0
Device(config-if-vlan129)#end
```

#Configure the IP address of VLAN130 as 130.255.28.10/24.

```
Device#configure terminal
Device(config)#interface vlan 130
Device(config-if-vlan130)#ip address 130.255.28.10 255.255.255.0
Device(config-if-vlan130)#end
```

#Configure the IP address of VLAN131 as 131.255.28.10/24.

```
Device#configure terminal
Device(config)#interface vlan 131
Device(config-if-vlan131)#ip address 131.255.28.10 255.255.255.0
Device(config-if-vlan131)#end
```

Step 3: Configure the AAA authentication.

#On Device, enable the AAA authentication, adopt the RADIUS authentication mode, the RADIUS server address is 129.255.43.90/24, the key value is admin, and the priority is 1.

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication connection default radius
Device(config)#radius-server host 129.255.43.90 priority 1 key admin
```

Step 4: Configure the AAA server.

#On the AAA server, configure the user name, password, and key value as admin

(omitted).

Step 5: Configure the ordinary L3 Portal authentication.

#On Device, configure the Portal server named server1.

```
Device(config)# portal server server1 ip 129.255.43.99 key admin url http://129.255.43.99:8080/portal
```

#On Device, enable the ordinary L3 Portal authentication.

```
Device#configure terminal
Device(config)#interface vlan 128
Device(config-if-vlan128)#portal server server1 method layer3 ip
Device(config-if-vlan128)#exit
```

#Configure one secure channel named channel, permitting PC1 and PC2 to access Update Server.

```
Device#configure terminal
Device(config)#hybrid access-list advanced channel
Device(config-adv-hybrid-nacl)#permit ip any any host 130.255.28.20 any
```

#Apply the secure channel named channel.

```
Device#configure terminal
Device(config)#global security access-group channel
Device(config)#exit
```

Step 6: Configure the Portal server.

#On the Portal server, configure the IP address, Device adderss and key value of PC1 as admin (omitted).

Step 7: Check the result.

```
#Query the configuration information of the secure channel.
Device#show portal global config
 portal global configuration information:
 authentication method list   : default
 accounting method list       : default

 global security access-group : channel
```

#Before passing the authentication, PC1 can access Update Serrver, and cannot access IP Network.

#PC1 can pass the authentication and can access Update Server and IP Network. PC2 can access Update Server, and cannot access IP Network.

```
Device#show portal user
--------------------
NO 1:IP_ADDRESS= 128.255.36.1  STATUS=    Authorized    USER_NAME=  admin
   INTERFACE=  vlan128      CTRL_METHOD= L3_IP        AUTH_STATE=  AUTHENTICATED
   BACK_STATE= AAA_SM_IDLE

 Total: 1   Authorized: 1   Unauthorized/Guest/Critical: 0/0/0
```

9.14 Trusted Device Access

9.14.1 Overview

To protect the core network from being illegally accessed, the edge device of the core network must have high security. This requires that other network devices connected to the edge device of the core network must be a clear trusted device. The trusted device access function is based on a mature 802.1X protocol to prevent unauthorized devices from accessing the core network. The basic network topology, as shown in Figure 7-1, includes three entities: the Access Device, the Authentication System, and the Authentication Server System.

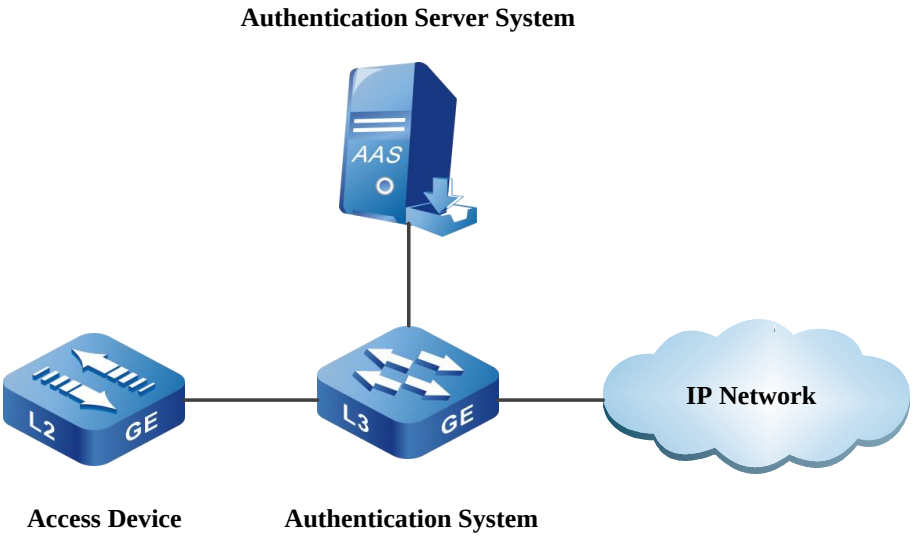


Figure 264 The access topology diagram of the trusted device

The specific method of the trusted device access is as follows:

- Enable the access function of the trusted device on the access device, and configure the required identity credentials and related parameters on the access device and authentication server.
- Enable the 802.1X device authentication function on the authentication device, the port connected to the access device becomes the controlled port waiting for the access of the access device.
- The access device automatically initiates the 802.1X authentication after connecting the authentication device. After passing the 802.1X authentication, the authentication device opens the controlled port, and the access device is connected to the network successfully.
- The access device regularly performs the keepalive authentication for the authentication device by the set the keepalive period of the authentication device.

9.14.2 Trusted Device Access Function Configuration

Table 1191 Trusted device access function configuration list

Configuration task	
Configure the access of the trusted device	Configure the user name and password of the trusted device access
	Configure the user name format of the trusted device access
	Configure the trigger period of the trusted device access
	Enable the access function of the trusted device
Configure the 802.1X device authentication	Enable the authentication function of the 802.1X device
	Configure the keepalive period of the 802.1X device authentication

9.14.2.1 Configure Trusted Device Access

Configuration Condition

None

Configure User Name and Password of Trusted Device Access

To connect the access device to the network successfully, you need to configure the user name and password of the trusted device access on the port connected to the authentication device. The configured user name and password are sent to the authentication device for authentication as the authentication credential of the access device via the 802.1X protocol (MD5-Challenge mode)

Table 1192 Configure the user name and password of the trusted device access

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 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	interface link-aggregation *link-aggregation-id*	
Configure the user name and password of the trusted device access	dot1x client user *username* password 0 *password*	Mandatory By default, the port is not configured with the user name or password of the trusted device access.

Note

- In one port, you can only configure one user name and password for the device access. In one port, the new user name and password will cover the original user name and password in the port.

Configure Access User Name Format of Trusted Device

802.1X authentication determines whether the peer initiating the authentication is a device or a terminal by whether the protocol packet EAP-Response/Identity carries the device ID. When the access user name of the trusted device in one port carries the device ID, the authentication initiated by the port is the 802.1X device authentication. When the access user name of the trusted device in one port does not carry the device ID, the authentication initiated by the port is the 802.1X terminal authentication.

Table 1193 Configure the user name format of the trusted device access

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 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	interface link-aggregation *link-aggregation-id*	
Configure the user name format of the trusted device access	dot1x client user-name-format { with-dev-flag | without-dev-flag }	Mandatory By default, the user name of the trusted device access in the port

Step	Command	Description
		carries the device ID.

Configure Trigger Period of Trusted Device Access

Before passing the authentication, the accessed device actively initiates the EAPoL-Start packet to perform the 802.1X device authentication according to the configured access trigger period, ensuring that the accessed device can connect the network fast.

Table 1194 Configure the trigger period of the trusted device access

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 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	interface link-aggregation *link-aggregation-id*	
Configure the trigger period of the trusted device access	dot1x client auth-interval *interval-value*	Mandatory By default, the trigger period of the trusted device access in the port is 15s.

Enable Access Function of Trusted Device

After enabling the access function of the device, the accessed device actively performs the 802.1X device authentication before passing the authentication. After passing the 802.1X device authentication, the authenticated device enables the controlled port, and the accessed device successfully connects the network.

Table 1195 Enable the access function of the trusted device

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 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	interface link-aggregation *link-aggregation-id*	
Enable the access function of the trusted device	dot1x client { enable | disable }	Mandatory By default, the access function of the trusted device in the port is disabled.

Note

- You cannot enable the access function and 802.1X authentication function of the trusted device on one port at the same time.
- You cannot enable the access function and MAC address authentication function of the trusted device on one port at the same time.
- You cannot enable the access function and secure channel authentication function of the trusted device on one port at the same time.

9.14.2.2 Configure 802.1X Device Authentication

Configuration Condition

None

Enable the Authentication Function of 802.1X Device

To make the 802.1X device authentication function take effect on the authentication device, you need to enable the 802.1X authentication and 802.1X device authentication function at the same time. After the device authentication takes effect, the connected port of the authentication device and access device becomes the controlled port. After device authentication succeeds, the authentication device enables the controlled port, and the access device connects the network successfully.

Table 1196 Enable the authentication function of the 802.1X device

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 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	interface link-aggregation *link-aggregation-id*	
Enable the 802.1X authentication	dot1x port-control { enable | disable }	Mandatory By default, the 802.1X authentication function in one port is disabled.
Enable the 802.1X device authentication	dot1x device-auth { enable | disable }	Mandatory By default, the 802.1X device authentication function in one port is disabled.

Note

- You cannot enable the authentication function and MAC address authentication function of the 802.1X device on one port at the same time.
- You cannot enable the authentication function and secure channel authentication function of the 802.1X device on one port at the same time.

Configure Keepalive Period of 802.1X Device Authentication

To detect whether the access device is online, after passing the authentication, the authentication device delivers the keepalive period of the configured 802.1X device authentication to the access device, and the access device initiates the keepalive authentication by the keepalive period. If the authentication device does not receive the keepalive authentication from the access device within three times of the keepalive period, it is regarded that the access device is not online, and change the port status to the controlled state.

Table 1197 Configure the keepalive period of the 802.1X device authentication

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 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	interface link-aggregation *link-aggregation-id*	
Configure the keepalive period	dot1x device-auth keepalive	Mandatory

Step	Command	Description
of the 802.1X device authentication	*period-value*	By default, the keepalive period of the 802.1X device authentication in one port is 600s.

9.14.2.3 Monitoring and Maintaining of Trusted Device Access

Table 1198 Monitoring and maintaining of the trusted device access

Command	Description
show dot1x client config { interface *interface-name* | link-aggregation *link-aggregation-id* }	Display the configuration information
show dot1x client user { interface *interface-name* | link-aggregation *link-aggregation-id* }	Display the access information
show dot1x user [*mac-address* | auth-type {device | user } | interface *interface-name* | link-aggregation *link-aggregation-id* | summary]	Display the user information

9.14.3 Typical Configuration Example of Trusted Device Access

Network Requirements

- The access device Device1 is connected to IP Network via the authentication device Device2; Device2 adopts the device authentication access control.
- The access device Device1 regularly initiates the keepalive authentication.
- During authentication, use the RADIUS authentication mode.
- After passing the access device authentication, PC permits accessing the network.

Network Topology

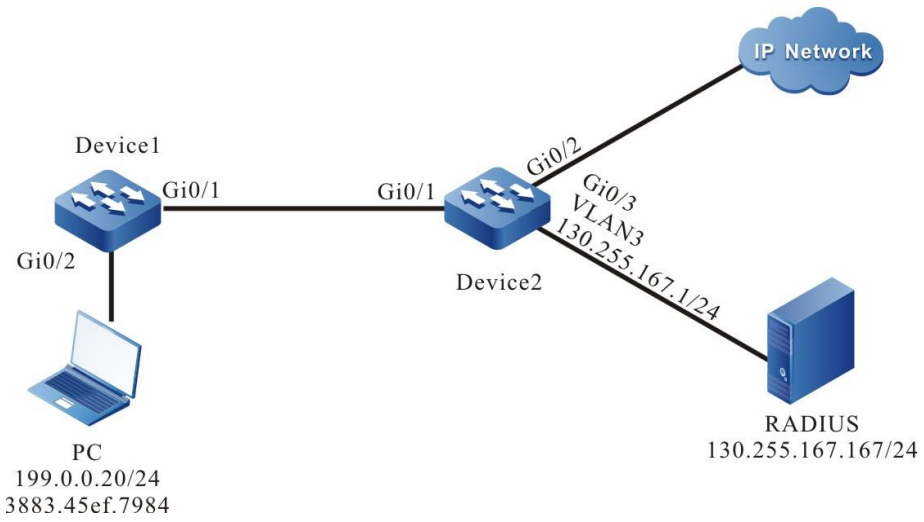


Figure 265 Networking of configuring trusted device access

Configuration Steps

Step 1: On Device1, configure the link type of the VLAN and port.

#On gigabitethernet 0/2 of Device1, configure the port link type as Access, permitting the services of VLAN2 to pass.

```
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

#On gigabitethernet 0/1 of Device1, configure the port link type as Hybrid, and the port is added to VLAN2 in the Tagged mode.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-range)#switchport mode hybrid
Device1(config-if-range)#switchport hybrid tagged vlan 2
Device1(config-if-range)#exit
```

Step 2: On Device2, configure the link type of the VLAN and port.

#On Device2, create VLAN2~VLAN3.

```
Device2#configure terminal
Device2(config)#vlan 2-3
Device2(config)#exit
```

#On gigabitethernet 0/1 of Device2, configure the port link type as Hybrid, and the port is added to VLAN2 in the Tagged mode.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-range)#switchport mode hybrid
Device2(config-if-range)# switchport hybrid tagged vlan 2
Device2(config-if-range)#exit
```

#On gigabitethernet 0/2-gigabitethernet 0/3 of Device2, configure the port link type as Access, permitting the services of VLAN2~VLAN3 to pass. (omitted)

Step 3 : Configure the interface IP address of Device2.

#On 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 4 : On Device2, configure the AAA authentication.

#On Device2, enable the AAA authentication, adopt the RADIUS authentication mode, the server key is admin, the priority is 1, and the address of the RADIUS server is 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 5 : Configure the AAA server.

On the AAA server, configure the user name, password and key as admin. (Omitted)

Step 6 : On Device1, configure the trusted device access.

#On Device1, configure the user name and password of the trusted device access authentication.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x client user admin password 0 admin
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, configure initiating the eapol-start packet actively with an interval of 10s to perform the 802.1X device authentication.

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x client auth-interval 10
Device1(config-if-gigabitethernet0/1)#exit
```

#On Device1, enable the access function of the trusted device.

```
Device1(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x client enable
Device2(config-if-gigabitethernet0/1)#exit
```

Step 7: On Device2, configure the 802.1X device authentication.

#On Device2, enable the 802.1X authentication.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#exit
```

#On Device2, enable the 802.1X device authentication.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x device-auth enable
Device2(config-if-gigabitethernet0/1)#exit
```

#On Device2, configure the keepalive period of the 802.1X device authentication as 120s.

```
Device2(config)#interface gigabitethernet 0/1
```

```
Device2(config-if-gigabitethernet0/1)#dot1x device-auth keepalive 120
Device2(config-if-gigabitethernet0/1)#exit
```

Step 8: Check the result.

#Before passing the access device authentication, PC cannot access network. After passing authentication, PC can access the network normally.

```
Device1#show dot1x client user
 Interface          : gi0/1
 Status             : Authorized
 State Machine State : AUTHENTICATED
 Keep Alive Interval : 120 sec (802.1X Server)


Device2#show dot1x user auth-type device
--------------------
NO 1  : MAC_ADDRESS= 3883.45ef.7984   STATUS=    Authorized   USER_NAME=  admin
       VLAN=      2            INTERFACE=  gi0/1       USER_TYPE=  DOT1X
       AUTH_STATE=  AUTHENTICATED    BACK_STATE=  IDLE        IP_ADDRESS=  Unknown
       Online time: 0 week 0 day 0 hour 0 minute 53 seconds

 Total: 1   Authorized: 1   Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

9.15 ACL Configuration

9.15.1 Overview

9.15.1.1 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 seven kinds, that is, IP standard ACL, IP extended ACL, MAC standard ACL, MAC extended ACL, Hybrid extended ACL, IPv6 standard ACL, and IPv6 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.
- IPv6 extended ACL: 7001-8000
- MPLS standard ACL: 8001-9000

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”.

9.15.1.2 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.

9.15.2 ACL Function Configuration

Table 1199 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 IPv6 standard ACL	Configure the IPv6 standard ACL
	Configure the IPv6 standard ACL named by

Configuration Task	
	numbers
Configure IPv6 extended ACL	Configure IPv6 extended ACL
	Configure IPv6 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
	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
	Configure IPv6 ACL to be applied to the port
	Configure IPv6 ACL to be applied to the interface

9.15.2.1 Configure IP Standard ACL

IP standard ACL makes the rules according to the source IP address to filter the packets.

Configuration Condition

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 1200 Configure the 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*] [log] [pbr-action-group *pbr-action-group-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*] [log] [pbr-action-group *pbr-action-group-name*]	Optional By default, the refuse rule of ACL is not configured.

Step	Command	Description
	[l3-action-group *l3-action-group-name*] [egr-action-group *egr-action-group-name*] [vfp-action-group *vfp-action-group-name*]	
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 1201Configure the 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-*	Mandatory By default, the IP standard ACL

Step	Command	Description
	addr source-wildcard | host *source-addr* } [time-range *time-range-name*] [log] [pbr-action-group *pbr-action-group-name*] [l3-action-group *l3-action-group-name*] [egr-action-group *egr-action-group-name*] [vfp-action-group *vfp-action-group-name*]	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.

9.15.2.2 Configure IP Extended ACL

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 Condition

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 1202 Configure the 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] [log] [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*] [vfp-action-group *vfp-action-*	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
	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] [log] [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*] [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 1203 Configure the 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] [log] [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*] [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.

Step	Command	Description
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.

9.15.2.3 Configure MAC Standard ACL

MAC standard ACL makes the rules according to the source MAC address to filter the packets.

Configuration Condition

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 1204 Configure the MAC standard ACL

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the MAC standard ACL	mac access-list standard { *access-list-number* |	Mandatory By default, the MAC

Step	Command	Description
	access-list-name }	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*] [log] [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*] [log] [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 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 1205Configure the 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*] [log] [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 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.

9.15.2.4 Configure MAC Extended ACL

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 Condition

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 1206 Configure the 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.

Step	Command	Description
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*] [log] [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* } { any | *destination-addr destination-wildcard* | host *destination-addr* } [ether-type *type*] [cos *cos*] [vlan-id *vlan*] [time-range *time-range-name*] [log] [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 1207 Configure the 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*] [log] [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.

Step	Command	Description
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.

9.15.2.5 Configure Hybrid Extended ACL

Hybrid extended ACL can make the classification rule according to the source MAC address, destination MAC address, Ethernet type, IP protocol type, source IP address, destination IP address, packet priority, VLAN ID, and 802.1p priority, so as to filter the packets.

Configuration Condition

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 Hybird extended ACL can only be applied globally, and can only filter the received packets.

Table 1208 Configure the 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 { any | *source-mac -addr source-wildcard* | host *source-mac-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* } [cos *cos*] [vlan-id *vlan*] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-action-group-name*] [ether-type] { *etherne-type* | *ipv4 protocol* } { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any | *destination -ip-addr destination -wildcard* | host *destination-ip-addr* }[precedence *precedence*] [tos *tos*] [dscp *dscp*] [fragments] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-action-group-name*]	Optional By default, the permit rule of ACL is not configured.

Step	Command	Description
Configure the refuse rule of ACL	[*sequence*] deny { any | *source-mac -addr source-wildcard* | host *source-mac-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* } [cos *cos*] [vlan-id *vlan*] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-action-group-name*] [ether-type] { *etherne-type* | *ipv4 protocol* } { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any | *destination -ip-addr destination -wildcard* | host *destination-ip-addr* }[precedence *precedence*] [tos *tos*] [dscp *dscp*] [fragments] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-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 **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 1209 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 } { any | *source-mac -addr source-wildcard* | host *source-mac-addr* } { any | *destination-mac-addr destination-wildcard* | host *destination-mac-addr* } [cos *cos*] [vlan-id *vlan*] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-action-group-name*] [ether-type] { *etherne-type* | *ipv4 protocol* } { any | *source-ip-addr source-wildcard* | host *source-ip-addr* } { any |	Mandatory By default, the Hybrid extended ACL named by numbers is not configured. The sequence range of the Hybrid extended ACL is 5001-6000.

Step	Command	Description
	destination -ip-addr destination -wildcard | host *destination-ip-addr* }[precedence *precedence*] [tos *tos*] [dscp *dscp*] [fragments] [time-range *time-range-name*] [egr-action-group *egr-action-group-name*] [l3-action-group *l3-action-group-name*]	
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.

9.15.2.6 Configure IPv6 Standard ACL

IPv6 standard ACL makes the classification rules according to the source IPv6 address to filter the packets.

Configuration Condition

None

Configure IPv6 Standard ACL

IP standard ACL name can use the numbers, and also can use the customized character string. When using the numbers, you can configure the maximum number of

the ACLs. When 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 1210 Configure the IPv6 standard ACL

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the IPv6 standard ACL	ipv6 access-list standard { *access-list-number* | *access-list-name* }	Mandatory By default, the IPv6 standard ACL is not configured.
Configure the permit rule of ACL	[*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, 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*] [pbr-action-group *pbr-action-group-name*]	Optional By default, do not configure the ACL refuse rule.
Configure the ACL remarks	[*sequence*] remark *comment*	Optional By default, do not configure the ACL rule remarks.

Note

- When using the **ipv6 access-list standard** command to create the IPv6 standard ACL, the ACL can be created only after configuring the rules in the IPv6 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 the IPv6 Standard ACL Named by Numbers

The IPv6 standard ACL named by numbers can let the user identify the type of the ACL quickly. However, the IPv6 standard ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 1211 Configure the IPv6 standard ACL named by numbers

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the IPv6 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*] [pbr-action-group *pbr-action-group-name*]	Mandatory By default, the IPv6 standard ACL named by numbers is not configured. The sequence range of the IPv6 standard ACL is 6001-7000.
Configure the remarks of the IPv6 standard ACL named by numbers	access-list *access-list-number* remark *comment*	Optional By default, the remarks of the IPv6 standard ACL named by

Step	Command	Description
		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.

9.15.2.7 Configure IPv6 Extended ACL

IPv6 extended ACL can make the classification rule according to the IPv6 protocol number, source IPv6 address, destination IPv6 address, source TCP/UDP port number, destination TCP/UDP port number, packet priority, fragment tag, and TCP tag, so as to filter the packets.

Configuration Condition

None

Configure IPv6 Extended ACL

IPv6 extended ACL name can use the number and also can use the customized character string. If the IPv6 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.

Table 1212 Configure the IPv6 extended ACL

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the IPv6 extended ACL	ipv6 access-list extended { *access-list-number* | *access-list-name* }	Mandatory By default, IPv6 extended

Step	Command	Description
		ACL is not configured.
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*] [pbr-action-group *pbr-action-group-name*] [l3-action-group *l3-action-group-name*] [egr-action-group *egr-action-group-name*]	Optional By default, the permit rule of ACL is not configured.
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*] [pbr-action-group *pbr-action-group-name*] [l3-action-group *l3-action-group-name*] [egr-action-group *egr-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 **ipv6 access-list extended** command to create the IPv6 extended ACL, the ACL can be created only after configuring the rules in the IPv6 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 IPv6 Extended ACL Named by Numbers

The IPv6 extended ACL named by numbers can let the user identify the type of the ACL quickly. However, the IPv6 extended ACL named by numbers has some limitations. For example, the ACL quantity is limited.

Table 1213 Configure the IPv6 extended ACL named by numbers

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the 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*]	Mandatory By default, the IPv6 extended ACL named by numbers is not configured. The sequence range of the IPv6 extended ACL is 7001-8000.

Step	Command	Description
	[l3-action-group *l3-action-group-name*] [egr-action-group *egr-action-group-name*]	
Configure the remarks of the IPv6 extended ACL named by numbers	access-list *access-list-number* remark *comment*	Optional By default, the remarks of the IPv6 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.

9.15.2.8 Configure Commit Operation

The commit operation command is to confirm the configured ACL rules and confirm whether the added or deleted rules take effect. After adding or deleting ACL rules, you should perform the commit operation. Otherwise, the added or deleted rules will not take effect. When saving the configuration, uncommitted rules will not be saved to the startup file.

Configuration Condition

Configure ACL

Configure Commit Operation

After configuring the ACL rule, you need to perform the Commit operation to submit the added or deleted ACL rules.

Table 1214 Configure the Commit operation of the ACL rule

Step	Command	Description
Enter the ACL configuration mode	ip access-list standard { *access-list-number* | *access-list-name* }	Mandatory By default, do not configure the IP standard ACL. The number range of the IP standard ACL is 1-1000. ACL configuration mode is not limited to IP standard ACL, and the commit operation supports all ACL configuration modes.
Submit the ACL rule operation	commit	Mandatory By default, the added or deleted rule is not Commit.

9.15.2.9 Configure ACL Rule Quantity Limitation

Configuration Condition

None

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 1215 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 { enable | disable }	Mandatory By default, it is disabled, that is, the maximum number of the rules that can be configured in one ACL is not limited to1024.

9.15.2.10 Configure 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 domain can be bound with ACL or ACL rule, as the condition of whether ACL or ACL rule takes effect.

Configuration Condition

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 1216 Configure the 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 1217 Configure the periodical time segment

Step	Command	Description
Enter global configuration mode	configure terminal	-

Step	Command	Description
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 [*day-of-the-week*] [*hh*: *mm* [: *ss*]] to [*day-of-the-week*] [*hh*: *mm* [: *ss*]]	Either By default, do not configure periodical time segment. The former command can specify the time range as one day (such as Monday) or several days (such as Monday, Friday). The latter command can specify the time range as every day, weekend, or workday.
	[*sequence*] periodic { weekdays | weekend | daily } [*hh*: *mm* [: *ss*]] to [*hh*: *mm* [: *ss*]]	

Configure Absolute Time Segment

The absolute time segment means to take effect within the specified date and time range.

Table 1218 Configure the 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 1219 Configure the refresh period

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the refresh period of the time domain	set time-range frequency { *frequency-min* | seconds *frequency-sec*}	Mandatory The default value is 1 minute. The refresh period is the interval between two refreshes and the unit is minute or second.

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 1220 Configure the 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-number*	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 1221 Configure the time domain to be bound with the ACL rule

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"	-
Configure the binding with Hybrid extended ACL rule	Refer to "Configure Hybrid Extended ACL"	-
Configure the binding with IPv6 standard ACL rule	Refer to "Configure IPv6 standard ACL"	-
Configure the binding with IPv6 extended ACL rule	Refer to "Configure IPv6 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 1222 Configure the 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.
Configure the time domain to be bound with IPv6 ACL	ipv6 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 IPv6 ACL.

Note

- When the time domain bound with the ACL rule does not exist, the ACL rule is in the effective state.

9.15.2.11 Configure ACL Application

ACL can be applied globally, to VLAN, port and interface. IP ACL all can be applied to global ingress direction, VLAN, the ingress and egress of the port and interface; Hybrid ACL can be applied globally, and to the egress and ingress of the port and interface; MAC ACL can be applied to the ingress and egress of the port and

interface; IPv6 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 L3 forwarding packets.

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, first match the permit packet with high priority; for the packet whose filter result is deny, directly drop it.

Configuration Condition

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 1223 Configure IP ACL to be applied to the port

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		port. After entering the aggregation group configuration mode, the subsequent configuration 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 IPv6 ACL to Be Applied to Port

Apply IPv6 ACL to the port. The packet passing the port is analyzed and processed according to IPv6 ACL.

Table 1224 Configure IPv6 ACL to be applied to the port

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 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
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
		group.
Configure IPv6 ACL to be applied to the port	ipv6 access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, IPv6 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 1225 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	interface 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 HYBRID ACL to Be Applied to Port

Apply HYBRID ACL to the port. The packet passing the port is analyzed and processed according to HYBRID ACL.

Table 1226 Configure HYBRID 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	interface link-aggregation *link-aggregation-id*	
Configure HYBRID ACL to be applied to the port	hybrid access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, HYBRID 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 VLAN is analyzed and processed according to IP ACL.

Table 1227 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, IP ACL is not applied to VLAN.

Note

- If ACL applied to the VLAN does not exist, all packets passing the VLAN are permitted.

Configure MAC ACL to Be Applied to VLAN

Apply MAC ACL to the VLAN. The packet passing the VLAN is analyzed and processed according to MAC ACL.

Table 1228 Configure MAC ACL to be applied to VLAN

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	-
Configure MAC ACL to be applied to VLAN	mac access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, MAC ACL is not applied to VLAN.

Note

- If ACL applied to the VLAN does not exist, all packets passing the VLAN are permitted.

Configure IPv6 ACL to Be Applied to VLAN

Apply IPv6 ACL to the VLAN. The packet passing the VLAN is analyzed and processed according to IPv6 ACL.

Table 1229 Configure IPv6 ACL to be applied to VLAN

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	-
Configure IPv6 ACL to be applied to VLAN	ipv6 access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, IPv6 ACL is not applied to VLAN.

Note

- If ACL applied to the VLAN does not exist, all packets passing the VLAN are permitted.

Configure MAC ACL to Be Applied to VLAN RANGE

Apply MAC ACL to VLAN RANGE. The packets passing VLAN RANGE are analyzed and processed according to MAC ACL.

Table 1230 Configure MAC ACL to be applied to VLAN RANGE

Step	Command	Description
Enter global configuration	configure terminal	-

Step	Command	Description
mode		
Configure MAC ACL to be applied to VLAN RANGE	mac access-group { *access-list-number* | *access-list-name* } { in | out } vlan range <1-4094>	Mandatory By default, MAC ACL is not applied to VLAN RANGE.

Note

- If ACL applied to VLAN RANGE does not exist, all packets passing the VLAN RANGE are permitted.

Configure IP ACL to Be Applied to VLAN RANGE

Apply IP ACL to VLAN RANGE. The packets passing VLAN RANGE are analyzed and processed according to IP ACL.

Table 1231 Configure IP ACL to be applied to VLAN RANGE

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure IP ACL to be applied to VLAN RANGE	ip access-group { *access-list-number* | *access-list-name* } { in | out } vlan range <1-4094>	Mandatory By default, IP ACL is not applied to VLAN RANGE.

Note

- If ACL applied to VLAN RANGE does not exist, all packets passing the VLAN RANGE are permitted.

Configure IPv6 ACL to Be Applied to VLAN RANGE

Apply IPv6 ACL to VLAN RANGE. The packets passing VLAN RANGE are analyzed and processed according to IPv6 ACL.

Table 1232 Configure IPv6 ACL to be applied to VLAN RANGE

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure IPv6 ACL to be applied to VLAN RANGE	ipv6 access-group { *access-list-number* | *access-list-name* } { in | out } vlan range <1-4094>	Mandatory By default, IPv6 ACL is not applied to VLAN RANGE.

Note

- If ACL applied to VLAN RANGE does not exist, all packets passing the VLAN RANGE are permitted.

Configure MAC ACL to Be Applied to L3 Interface VLAN RANGE

Apply MAC ACL to L3 interface VLAN RANGE. The packets passing L3 interface VLAN RANGE are analyzed and processed according to MAC ACL.

Table 1233 Configure MAC ACL to be applied to L3 interface VLAN RANGE

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure MAC ACL to be applied to L3 interface VLAN RANGE	mac access-group { *access-list-number* | *access-list-name* } { in | out } interface vlan range <1-4094>	Mandatory By default, MAC ACL is not applied to L3 interface VLAN RANGE.

Note

- If ACL applied to L3 interface VLAN RANGE does not exist, all packets passing the VLAN RANGE are permitted.

Configure IP ACL to Be Applied to L3 Interface VLAN RANGE

Apply IP ACL to L3 interface VLAN RANGE. The packets passing L3 interface

VLAN RANGE are analyzed and processed according to IP ACL.

Table 1234 Configure IP ACL to be applied to L3 interface VLAN RANGE

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure IP ACL to be applied to L3 interface VLAN RANGE	ip access-group { *access-list-number* | *access-list-name* } { in | out } interface vlan range <1-4094>	Mandatory By default, IP ACL is not applied to L3 interface VLAN RANGE.

Note

- If ACL applied to L3 interface VLAN RANGE does not exist, all packets passing the VLAN RANGE are permitted.

Configure IPv6 ACL to Be Applied to L3 Interface VLAN RANGE

Apply IPv6 ACL to L3 interface VLAN RANGE. The packets passing L3 interface VLAN RANGE are analyzed and processed according to IPv6 ACL.

Table 1235 Configure IPv6 ACL to be applied to L3 interface VLAN RANGE

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure IPv6 ACL to be applied to L3 interface VLAN RANGE	ipv6 access-group { *access-list-number* | *access-list-name* } { in | out } interface vlan range <1-4094>	Mandatory By default, IPv6 ACL is not applied to L3 interface VLAN RANGE.

Note

- If ACL applied to L3 interface VLAN RANGE does not exist, all packets passing the VLAN RANGE 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 1236 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 1237 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 | out }	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.

Configure IP ACL to Be Applied to an Interface

Apply IP ACL to an interface. The packet passing the port is analyzed and processed according to IP ACL.

Table 1238 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*	-
Configure IP ACL to be applied to the interface	ip access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, IP ACL is not applied to the interface.

Note

- If the ACL applied to the interface does not exist, all packets passing the interface are permitted.

Configure MAC ACL to Be Applied to an Interface

Apply MAC ACL to an interface. The packet passing the port is analyzed and processed according to MAC ACL.

Table 1239 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	mac access-group { *access-list-*	Mandatory

Step	Command	Description
applied to the interface	*number* | *access-list-name* } { in | out }	By default, MAC ACL is not applied to the interface.

Note

- If the ACL applied to the interface does not exist, all packets passing the interface are permitted.

Configure HYBRID ACL to Be Applied to an Interface

Apply HYBRID ACL to an interface. The packet passing the interface is analyzed and processed according to HYBRID ACL.

Table 1240 Configure HYBRID ACL to be applied to an interface

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure HYBRID ACL to be applied to an interface	hybrid access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, HYBRID ACL is not applied to the interface.

Note

- If the ACL applied to the interface does not exist, all packets passing the interface are permitted.

Configure IPv6 ACL to Be Applied to an Interface

Apply IPv6 ACL to an interface. The packet passing the interface is analyzed and processed according to IPv6 ACL.

Table 1241 Configure IPv6 ACL to be applied to an interface

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Apply IPv6 ACL to an interface	ipv6 access-group { *access-list-number* | *access-list-name* } { in | out }	Mandatory By default, IPv6 ACL is not applied to the interface.

Note

- If the ACL applied to the interface does not exist, all packets passing the interface are permitted.

9.15.2.12 Configure ACL Mode

There are two modes when the same ACL is applied to different ports. One is port mode. In the Port mode, the same ACL uses different ACL resources on different ports, and the traffic of different ports uses different resources to match. The other is bitmap mode. In the bitmap mode, the same ACL uses the same ACL resources on different ports, the port matching is realized by bitmap, and the traffic of different ports is matched by related resources. In this way, bitmap mode can save resources. By default, ACL is in port mode.

Configuration Condition

None

Configure ACL Mode

When the same ACL is used on different ports, the mode can be used to adjust whether the ACL separately delivers resources on the ports or whether the resources are shared by BitMap.

Table 1242 Configure the ACL mode

Step	Command	Description
Enter global configuration mode	configure terminal	-
Configure the ACL mode	acl mode { port | bitmap }	Mandatory By default, the ACL is in the Port mode.

9.15.2.13 ACL Monitoring and Maintaining

Table 1243 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 [vlan [in | out] | switchport [in | out | vfp]] | vlan [in | out] | vlan-range [in | out]]	Display the VLAN, port, global applied ACL, and interface VLAN information.
show ip access-list [*access-list-number* | *access-list-name*]	Display the IP ACL configuration information
show hybrid access-list [*access-list-number* | *access-list-name*]	Display the configuration information of Hybird extended, advanced ACL
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 IPv6 ACL configuration information
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
show time-range-state [*time-range-name*]	Display the time domain status information
show acl mode	Display the ACL mode information

9.15.3 ACL Typical Configuration Example

9.15.3.1 Configure IP Standard ACL

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

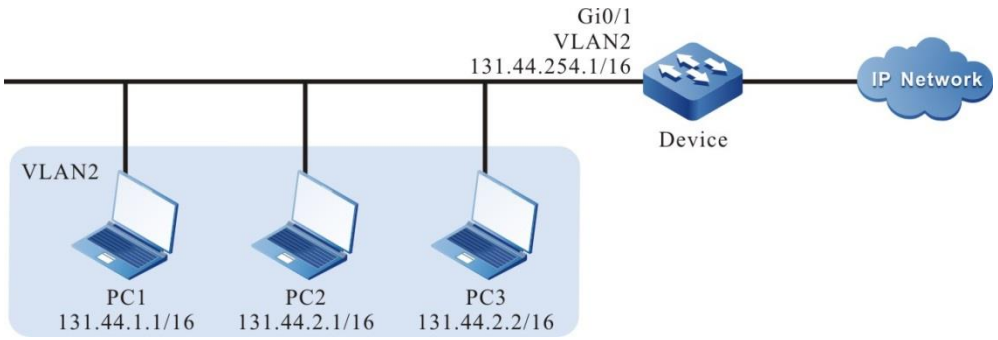


Figure 266 Networking of configuring IP standard ACL

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
```

#Submit the configured rule

```
Device(config-std-nacl)#commit
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
-----------Interface-----Bind-----Instance--------------
Interface VlanId---------Direction----AclType----AclName
```

```
Device#
```

Step 5: Check the result.

#PC1 can access IP Network; PC and PC3 cannot access IP Network.

9.15.3.2 Configure IP Extended ACL with Time Domain

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

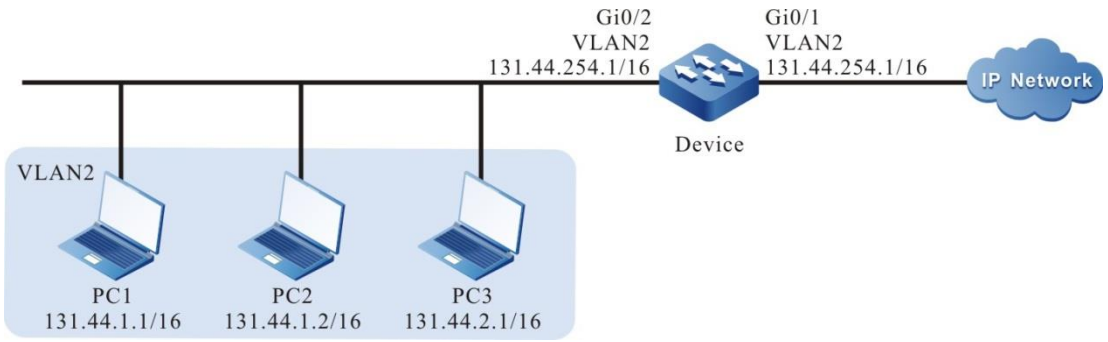


Figure 267 Networking of configuring IP extended ACL with time domain

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 08:00:00 to 18:00:00 every day.

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00:00 to 18:00:00
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 08:00:00 to 18:00:00 (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
```

#Submit the configured rule

```
Device(config-ext-nacl)#commit
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
gi0/1                OUT        IP        1001
-----------Interface-----Bind-----Instance--------------
Interface VlanId---------Direction----AclType----AclName
```

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.

9.15.3.3 Configure MAC Standard ACL

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

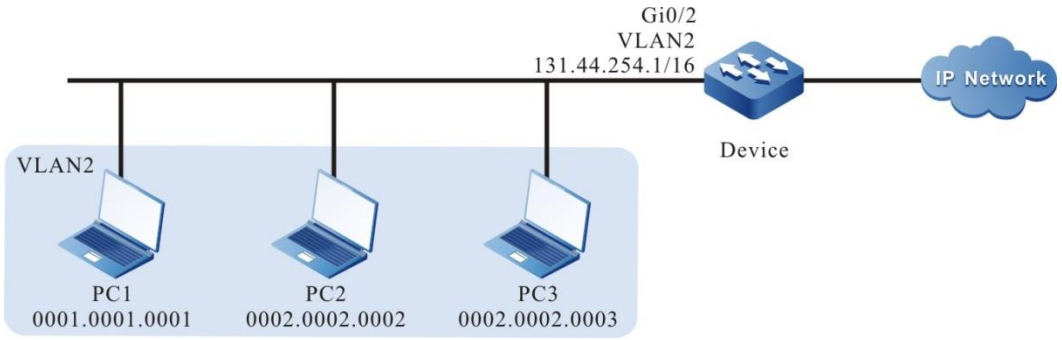


Figure 268 Networking of configuring MAC standard ACL

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
```

#Submit the configured rule

```
Device(config-ext-nacl)#commit
```

#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
-----------Interface-----Bind-----Instance--------------
Interface VlanId---------Direction----AclType----AclName
```

Step 5: Check the result.

#PC1 can access IP Network; PC2 and PC3 cannot access IP Network.

9.15.3.4 Configure MAC Extended ACL

Network Requirements

- PC1, PC2, and IP Phone are connected to IP Network via Device1.
- 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

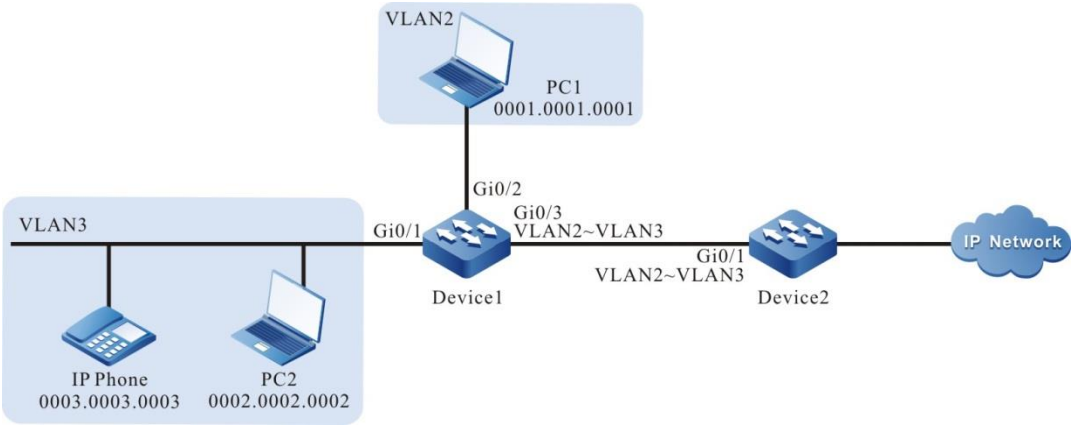


Figure 269 Networking of configuring the MAC extended ACL

Configuration Steps

Step 1: Configure the link type of VLAN and port on Device2.

#Create VLAN2 and VLAN3.

```
Devic2e#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit

Device2#configure terminal
Device2(config)#vlan 3
Device2(config-vlan3)#exit
```

#Configure the link type of port gigabitethernet0/1 as Trunk, permitting the services of VLAN2 and VLAN3 to pass.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk vlan 2-3
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
```

#Submit the configured rule

```
Device2(config-ext-nacl)#commit
```

#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.

```
Device#show acl-object interface
-----------Interface-----Bind-----Instance--------------
Interface----------------Direction----AclType----AclName
gi0/1              IN        MAC       3001
-----------Interface-----Bind-----Instance--------------
Interface VlanId---------Direction----AclType----AclName
```

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.

9.15.3.5 Configure Hybrid Extended ACL

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

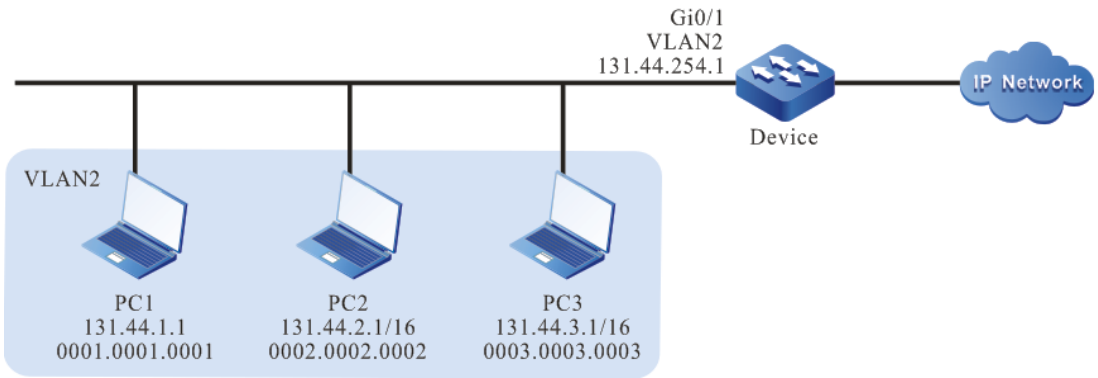


Figure 270 Networking of configuring Hybrid extended ACL

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, permitting PC1 to access IP Network in the defined time domain “time-range-work” range.

```
Device(config-hybrid-nacl)# permit host 0001.0001.0001 any ether-type ipv4 ip any any time-range time-range-work
```

#Configure the rule, preventing the segment 131.44.0.0/16 from accessing IP Network.

```
Device(config-hybrid-nacl)# deny any any ether-type ipv4 ip 131.44.0.0 0.0.255.255 any
```

#Configure the rule, permitting all packets from IP Network to pass Device.

```
Device(config-hybrid-nacl)# permit any any ether-type ipv4 ip any any
```

#Submit the configured rule

```
Device(config-hybrid-nacl)#commit
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 permit host 0001.0001.0001 any ether-type ipv4 ip any any time-range time-range-work (active)
 20 deny any any ether-type ipv4 ip 131.44.0.0 0.0.255.255 any
 30 permit any any ether-type ipv4 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 cannot access IP Network.

9.16 Attack Defense

9.16.1.1 Overview

Attack defense is an important function to maintain network security. It judges whether the packet has attack characteristics by analyzing the packet content passing through the device, and implements certain preventive measures for the packet with attack characteristics according to the configuration, such as intercepting the attack packet, recording the attack packet log, adding the attack source to the blacklist, etc. By configuring the attack defense function on the device, on the one hand, it can avoid the abnormality of the device due to network attack and improve the anti-attack ability of the device; On the other hand, it can intercept the attack traffic forwarded by the device to prevent other devices on the network from working normally due to attacks.

9.16.2 Attack Defense Function Configuration

Table 1244 Attack defense function configuration list

Configuration Tasks	
Configure single-packet attack defense function	The hardware detection supports configuring intercepting frag-icmp, icmp-large, icmpv6-large, ping-of-death, smurf, src-dst-mac-equal, src-dst-ip-equal, src-dst-port-equal, tcp-flag-seq-zero, tcp-hdr-incomplete, tcp-invalid-flag, tcp-syn-fin, smac-zero, invalid-ttl, smac-non-unicast attack packets, and the actual results are based on the capability set of each chip. The software configures interrupting fraggle, fragment, tcp-land, REDIRECT, UNREACH, ECHOREPLY, SOURCEQUENCH, ECHO, ROUTERADVERT, ROUTERSOLICIT, TIMXCEED, PARAMPROB, TSTAMP, TSTAMPREPLY, IREQ, IREQREPLY, MASKREQ, MASKREPLY, small-packet, icmp code none-zero, tear-drop attack packets.

Configure flood attack defense function	Configure intercepting tcp syn, tcp syn-ack, tcp ack, tcp fin, tcp rst, tcp urg, tcp port, udp, udp port, icmp, icmpv6, dns, http, ip types of flood attack packets
Configure scan attack defense function	Configure intercepting ip scan, port scan attack packets
Configure URPF attack defense function	Configure URPF check function
Configure the blacklist function	Configure the blacklist function to drop the packets of the corresponding source address
Configure the whitelist function	Configure the whitelist based on source IP and MAC address for exemption

Note: The intercepted packets configured by the software on the switch is only valid for the packet to the local machine.

9.16.2.1 Configure Single-Packet Attack Defense Function

Single-packet attack defense refers to judging whether the packet is aggressive by analyzing the characteristics of the packet passing through the device. Generally, it is only effective for the incoming packet with attack defense policy. After the single-packet attack defense function is configured, if the device detects that a packet is aggressive, it will output an alarm log, discard the packet, and make packet discarding statistics.

Configuration Conditions

None

Configure Intercepting Different Kinds of Single-packet Attack Defense Function

When an aggressive packet of the configured type is detected, the packet will be discarded and the discarded packet statistics will be carried out.

Table 1245 Configure the single-packet attack list

Step	Command	Description
Enter the global	configure terminal	-

configuration mode		
Configure to intercept the specified type of single packet attack message	anti-attack detect { fraggle | frag-icmp | icmp-large | icmpv6-large | ping-of-death | src-dst-ip-equal | src-dst-mac-equal | src-dst-port-equal | smurf | tcp-flag-seq-zero | tcp-hdr-incomplete | tcp-invalid-flags | tcp-land | tcp-syn-fin | tear-drop | smac-zero | invalid-ttl | smac-non-unicast } anti-attack drop { fragment [max-off *max-off*] | small-packet [*mini-length*] | icmp { type { REDIRECT | UNREACH | ECHOREPLY | SOURCEQUENCH | ECHO | ROUTERADVERT | ROUTERSOLICIT | TIMXCEED | PARAMPROB | TSTAMP | TSTAMPREPLY | IREQ | IREQREPLY | MASKREQ | MASKREPLY} | code none-zero }} anti-attack subnet-broadcast masklen *length*	Mandatory By default, the value of *max-off* is 65535; the value of *mini-length* is 64. When single packet attack prevention is configured by default, packet detection with this feature is not enabled except smac-non-unicast.

Configure Single-Packet Attack Defense Log Record

When the device detects the single-packet attack, it discards the packet and logs it at the same time.

Table 1246 Configure the single-packet attack log output

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the single-packet attack type of log output	attack-defense action logging detect	Mandatory By default, do not enable the single-packet attack defense log.

9.16.2.2 Configure Flood Attack Defense Function

Flood attack is mainly used to protect the server from the impact of large traffic packets. It is generally applied to the interface of the device connected to the external network, and is only effective for the incoming packet on the interface with attack defense policy. After the flooding attack defense policy is applied to the interface, the interface is in the attack detection state. When it detects that the rate of a certain type of packets continues to exceed the specified trigger threshold, it considers that the interface has been flooded, enters the attack defense state, and starts the corresponding defense policy according to the configuration (output the alarm log, discard the packet, and add the attack source to the dynamic blacklist, where the blacklist takes effect after the traceability function is configured). When the device detects that the packet traffic of this type is lower than the threshold for 5 seconds or the generated dynamic blacklist is aged, release the attack state and stop executing attack defense measures.

Configuration Conditions

- It is necessary to configure the attack defense policy, and configure the flood attack defense in the policy configuration mode.
- It is necessary to apply the attack defense policy globally or in the interface to enable the flood attack defense detection in the policy.

Configure to Intercept Different Kinds of Flood Attack Defense

When the packet configured with flood detection type exceeds the threshold, take the corresponding preventive measures.

Table 1247 Configure the flood attack defense

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the policy configuration mode	attack-defense policy *policy*	Mandatory
Configure flood detection	detect { tcp-syn | tcp-ack |	Mandatory

type and defense action	tcp-syn-ack | tcp-fin | tcp-rst|tcp-urg | tcp { port [*port-number* | bgp| ftp| ldp | ssh | syslog | telnet] } | udp {port [*port-number* | snmp | syslog | tftp] } | icmp | icmpv6 | dns | http | ip } flood threshold *threshold-value* action { drop | blacklist }*	By default, the corresponding type of flood attack detection is not enabled.

Configure Backtracking Attack Source Function during Flood Attack Detection

Trace the source of packets configured with flood attack defense type, and count the number of packets based on each source address.

Table 1248 Configure the flood attack defense tracking function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the policy configuration mode	attack-defense policy *policy*	Mandatory
Configure the flood attack defense tracking function	trace-type {source-ip | source-mac} max-count *max-source-number*	Mandatory By default, the single source threshold is not checked according to the source address *max-source-number* configures the number of flood detection traceability. The source address nodes exceeding the number of traceability will not be traced

Configure to Apply Attack Defense Policy Globally

The configuration of flooding attack is implemented based on policy, and the

configuration takes effect when the policy is applied globally.

Table 1249 Configure to apply the attack defense policy globally

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure to apply the attack defense policy globally	attack-defense global apply policy *policy-name*	Mandatory By default, no attack defense policies are applied globally.

Configure to Apply Attack Defense Policy in the Interface

The configuration of flooding attack is based on policy, and the configuration takes effect when the policy is applied. The policy can be applied separately based on the port or interface. If the global applied policy and the configuration under the port/interface exist at the same time, the configuration under the port/interface takes precedence.

Table 1250 Configure to apply the attack defense policy in the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the interface to apply the attack defense policy	attack-defense apply policy *policy-name*	Mandatory By default, the interface does not apply the policy separately.

Configure Flood Attack Defense Log Records

When the device detects a flood attack, it takes defense policy and records the log at the same time.

Table 1251 Configure to output flood attack logs

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Configure to output flood attack logs	attack-defense action logging flood	Mandatory By default, do not enable the flood attack defense log.

9.16.2.3 Configure Scan Attack Defense Function

Scanning attack defense mainly detects the detection behavior of network users by monitoring the rate of connection to the target system to prevent them from detecting the network state. It is generally applied to the interface of the device connected to the external network, and is only effective for the incoming packets on the interface where the attack defense policy is applied.

After scanning attack defense is configured, when the number of IPs accessed in the network or the number of ports accessed on a device exceeds the threshold, it is considered that a scanning attack has occurred in the network, the attack source is automatically detected and added to the dynamic blacklist, and the scanning attack defense log is output according to the configuration.

Configuration Conditions

- The attack defense policy needs to be configured. Scan the attack defense configuration in the policy configuration mode.
- Attack defense policy needs to be applied globally or on the interface to enable scanning attack defense detection in the policy.

Configure Scanning Attack Defense Function

When the scan attack defense level is configured and the number of accessed destinations addresses or ports of a destination address in the network exceeds the threshold, the scanning attack log is output or the attack source is added to the blacklist according to the configuration.

High indicates high-level defense, the number of destination IP addresses allowed to be accessed at the same time is 16, and the number of ports allowed to be accessed

at the same destination address is 4; Medium refers to medium level defense, the number of destination IP addresses allowed to be accessed at the same time is 32, and the number of ports allowed to be accessed at the same destination address is 8; Low indicates low-level defense, the number of destination IP addresses allowed to be accessed at the same time is 64, and the number of ports allowed to be accessed at the same destination address is 16.

Table 1252 Configure scanning attack defense function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the policy configuration mode	attack-defense policy *policy*	Mandatory
Configure scanning attack defense function	detect scan level {high | medium | low} action blacklist	Mandatory By default, do not enable the scanning attack detection.

Configure Scan Attack Defense Log Records

Record the log when the device detects a scan attack.

Table 1253 Configure to output the scan attack log

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure to output the scan attack log	attack-defense action logging scan	Mandatory By default, do not enable scan attack defense log.

9.16.2.4 Configure URPF Attack Defense Function

URPF is a unicast reverse path forwarding technology, used to prevent attacks based on source address spoofing, such as DoS (denial of service) attacks based on source address spoofing and DDoS (distributed denial of service) attacks.

Configuration Conditions

- You need to enable the URPF function globally to make the URPF detection effective.

Configure Global URPF Function

After enabling the URPF function globally, the URPF function on the interface can take effect.

Table 1254 Configure the global URPF function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the global URPF function	**ip urpf**	Mandatory By default, do not enable the URPF function globally.

Configure URPF Searching Default Route Function

When URPF finds the source route, it releases the packet that finds the source route as the default route by enabling the default route function.

Table 1255 Configure URPF to permit default route

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure URPF to permit the default route	ip urpf allow-default-route	Mandatory By default, do not enable the function of checking the default route.

Configure URPF in Interface

URPF supports strict and loose modes. In the loose mode, URPF searches the route table for the source address of the received packet. If a route is found, the packet is allowed to pass through; In strict mode, the packet is allowed to pass only when the route is found and the outgoing interface is the same as the receiving interface of the

packet.

Table 1256 Configure the URPF check on the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the URPF check on the interface	ip urpf { loose | strict }	Mandatory By default, the interface URPF function is not enabled.

Configure URPF Defense Log Records

When the device detects the URPF attack, perform the log recording.

Table 1257 Configure the URPF log output

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the URPF log output	attack-defense action logging urpf	Mandatory By default, do not enable the URPF attack defense log.

9.16.2.5 Configure Blacklist Function

Blacklist function is an attack defense feature that filters packets according to the source IP or IPv6 or MAC address of the packet. Compared with the packet filtering function based on ACL (access control list), the way of packet matching in blacklist is simpler, which can realize high-speed filtering and effective shielding of packets. Blacklists can be added or deleted dynamically by the device or manually by the user.

Configuration Conditions

None

Configure Static Blacklist

The dynamic blacklist is dynamically added by flood attack defense, scanning attack defense and other functions, and the static blacklist is manually configured by the user. The blacklist on the routing device is implemented by software.

Table 1258 Configure the static blacklist

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the static blacklist	blacklist {ip *ip-address* | ipv6 *ipv6-address* | mac *mac-address* }	Mandatory By default, do not configure the static blacklist.

Configure Aging Time of Dynamic Blacklist

Table 1259 Configure the aging time of the dynamic blacklist

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the aging time of the dynamic blacklist	blacklist dynamic aging-time *time*	Mandatory By default, do not configure the aging time of the dynamic blacklist, but use the default time 120s.

9.16.2.6 Configure Whitelist Function

The whitelist function is an attack prevention feature that releases packets according to the source IP or MAC address of the packet. If a whitelist is set up, the users in the whitelist (source IP address and source MAC address) will pass first to

avoid server accidental injury. The whitelist is manually added and deleted by the user.

Configuration Conditions

None

Configure Whitelist

The whitelist is manually configured by the user.

The whitelist on the switching device is implemented by ACL and software.

Table 1260 Configure the whitelist

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the whitelist	whitelist { ip *ip-address* | mac *mac-address* }	Mandatory By default, do not configure the whitelist.

9.16.2.7 Attack Defense Monitoring and Maintaining

Table 1261 Attack defense monitoring and maintaining

Command	Description
clear attack-defense nullscan stastiscs	Clear the NULL SCAN statistics information
clear anti-attack detect statistic teardrop	Clear the teardrop attack statistics information
clear anti-attack detect statistic [member *member-ID*]	Clear the single-packet attack statistics information
clear attack-defense trace stastiscs	Clear the traceability entry statistics information
clear attack-defense flood stastiscs	Clear the flood attack entry statistics information
clear blacklist dynamic { ip [*ip-address*] | ipv6 [*ipv6-address*] | mac [*mac-address*] } [member	Clear the dynamic blacklist on the board card

member-ID]	
show anti-attack detect statistic [member *member-ID*]	Display the single-packet attack statistics information
show attack-defense applied policy	Display the current global applied attack defense policy
show attack-defense policy [*policy-name*]	Display the attack defense policy configuration
show attack-defense flood [member *member-ID*] [interface *interface-name*]	Display the Flood attack defense status
show attack-defense scan { ip-scan | ipv6-scan | port-scan | ipv6-port-scan } [member *member-ID*]	Display the scan attack defense status
show attack-defense scan { statistic | ipv6-statistic } [member *member-ID*] interface *interface-name*	Display the scan attack defense status on the specified interface
show attack-defense trace [member *member-ID*] [interface *interface-name*]	Display the attack trace status
show blacklist config	Display the blacklist configuration information
show blacklist dynamic { ip | ipv6 | mac } [member *member-ID*]	Display the dynamic blacklist information
show attack-defense nullscan stastiscs [member *member-ID*]	Display the NULL SCAN statistics information
show running-config attack-defense interface	Display the security configuration in the interface (including interface, port, L2 vlan interface)
show anti-attack detect statistic teardrop	Display the teardrop statics information

9.16.3 Attack Defense Typical Configuration Example

9.16.3.1 Configure Single-packet Attack Detection

Network Requirements

- The attacker and PC access Device via the interface.
- Device configures the single packet attack detection function, alarms when

an attack packet is detected, and discards the attack packet. Take the common Fraggle attack and Land attack as examples.

Network Topology

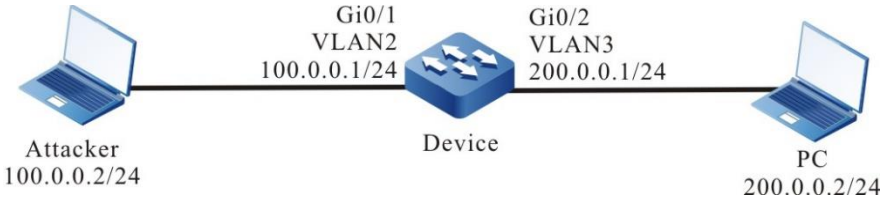


Figure 271 Networking of configuring single-packet attack detection

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. It is required that the PC can access IP Network via Device (omitted).

Step 3: On Device, configure the Fraggle, Land attack detection function, and enable the single-packet attack log switch.

#Configure the Fraggle attack detection.

```
Device#configure terminal
Device(config)#anti-attack detect fraggle
```

#Configure the Land attack detection.

```
Device(config)#anti-attack detect tcp-land
```

#On Device, open the single-packet attack log switch.

```
Device(config)#attack-defense action logging detect
```

Step 4: Check the result.

#When the attacker initiates Fraggle and land attacks for the PC, if this function is not configured, the attack packet can be captured on the PC. After configuring this function, the attack packet cannot be captured on the PC. View the log and statistics on the device.

#When Device receives the Fraggle attack, output the following log information:

```
%ANTIATTACK-DETECT_ATTACK_I-4:interface vlan2 detect single-packet attack, type fraggle.
```

#When Device receives the Land attack, output the following log information:

```
%ANTIATTACK-DETECT_ATTACK_I-4:interface vlan2 detect single-packet attack, type tcp-land.
```

#On the Device, execute the **show anti-attack detect statistic** command to view the statics information of the dropped attack packets.

```
Device#show anti-attack detect statistic
    detect-type            DropCount
    ------------------------------------------------
    fraggle              87
    fragment              0
    frag-icmp             0
    tcp-land            456
    REDIRECT              0
    UNREACH               0
    ECHOREPLY             0
    SOURCEQUENCH            0
    ECHO                0
    ROUTERADVERT            0
    ROUTERSOLICIT           0
    TIMXCEED              0
    PARAMPROB               0
    TSTAMP                0
    TSTAMPREPLY             0
    IREQ                0
    IREQREPLY               0
    MASKREQ               0
    MASKREPLY               0
    small-packet          0
    none-zero             0
    invalid-ttl         0
```

Note

- The hardware processing single packet attack detection on the switch is effective for both forwarded and local packets, and will not generate logs or statistics; The single packet attack detection processed by the software is only effective for the local packet, with log output and statistical

information.

9.16.3.2 Configure flood Attack Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.
- Device configures the flood attack detection function. When the corresponding characteristic type attack packet is detected, it outputs the alarm log and discards the attack packet. Take common TCP SYN Flood attacks and ICMP flood attacks as examples.

Network Topology

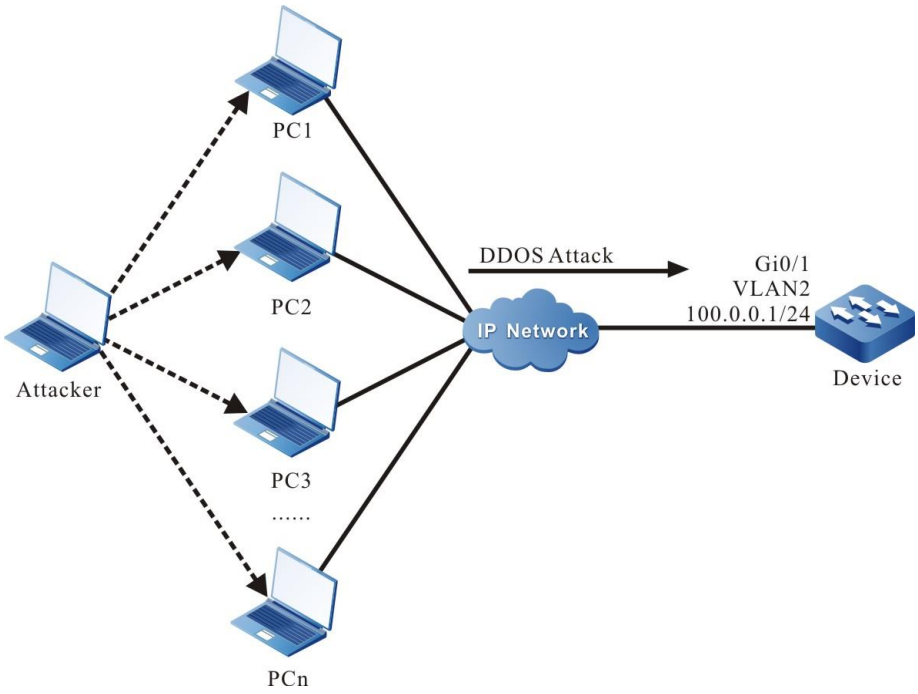


Figure 272 Networking of configuring flood attack detection

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. It is required that the PC can access IP Network via Device (omitted).

Step 3: Configure the attack defense policy a on Device, add the TCP SYN Flood and ICMP flood attack detection functions in the policy, and configure the attack traceability based on IP address.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect tcp-syn flood threshold 500 action drop
Device(config-anti-policy-a)#detect icmp flood threshold 500 action blacklist
Device(config-anti-policy-a)#trace-type source-ip max-count 5
Device(config-anti-policy-a)#exit
```

#On Device, globally apply attack defense policy a.

```
Device(config)#attack-defense global apply policy a
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 3: Check the result:

#View the currently applied attack defense policy on Device.

```
Device#show attack-defense applied policy
attack-defense policy a
 detect tcp-syn flood threshold 500 action drop
 detect icmp flood threshold 500 action blacklist
 trace-type source-ip max-count 5
```

#When an attacker initiates TCP SYN Flood and ICMP flood attacks on Device, view the flood attack log output on Device.

```
%ANTIATTACK-FLOOD_ATTACK_J-4:interface vlan2 detect attack, type tcp-syn.
%ANTIATTACK-FLOOD_ATTACK_J-4:interface vlan2 detect attack, type icmp, ipaddr 100.0.0.2.
```

#View the attack traceability table entry on Device.

```
Device#show attack-defense trace
  Trace Info:
  IpAddr, Interface
    Type          DropCount       Token          LastRecvTime
-------------------------------------------------------------------------------
--
  100.0.0.2, vlan2
    icmp          , 0             , 299          , Sun Apr 25 10:58:43 2021
```

```
    tcp-syn       , 0          , 349          , Sun Apr 25 10:58:43 2021
  100.0.0.5, vlan2
    icmp          , 0          , 392          , Sun Apr 25 10:58:43 2021
    tcp-syn       , 0          , 366          , Sun Apr 25 10:58:43 2021
  100.0.0.4, vlan2
    icmp          , 0          , 391          , Sun Apr 25 10:58:43 2021
    tcp-syn       , 0          , 351          , Sun Apr 25 10:58:43 2021
  100.0.0.3, vlan2
    icmp          , 0          , 391          , Sun Apr 25 10:58:43 2021
    tcp-syn       , 0          , 367          , Sun Apr 25 10:58:43 2021
  100.0.0.2, gigabitethernet0/1
      icmp            , 0             , 299           , Sun Apr 25 10:58:43 2021
      tcp-syn         , 0             , 349           , Sun Apr 25 10:58:43 2021
   100.0.0.5, gigabitethernet0/1
      icmp            , 0             , 392           , Sun Apr 25 10:58:43 2021
      tcp-syn         , 0             , 366           , Sun Apr 25 10:58:43 2021
   100.0.0.4, gigabitethernet0/1
      icmp            , 0             , 391           , Sun Apr 25 10:58:43 2021
      tcp-syn         , 0             , 349           , Sun Apr 25 10:58:43 2021
   100.0.0.3, gigabitethernet0/1
      icmp            , 0             , 391           , Sun Apr 25 10:58:43 2021
      tcp-syn         , 0             , 366           , Sun Apr 25 10:58:43 2021
```

#On Device, view the flood attack defense status information.

```
Device#show attack-defense flood
  Flood Info:
    Type          DropCount       Token         LastRecvTime
-------------------------------------------------------------------------------
--
  gigabitethernet0/1
    tcp-syn       , 1851          , 50          , Mon May 04 16:55:50 2020
    icmp          , 0             , 100         , Mon May 04 16:55:46 2020
```

#View the dynamic blacklist items generated by traceability on Device.

```
Device#show blacklist ip
  Blacklist Info:
  IpAddr,              CreateTime,             Agetime
-----------------------------------------------------------------------
  100.0.0.2          ,    Mon May 04 16:55:47 2020     , 93
```

9.16.3.3 Configure Scan Attack Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.

- Device configures the scanning attack detection function, outputs the alarm log when IP scanning or port scanning is detected, adds the attack source to the blacklist, and intercepts all packets of the attack source before the blacklist aging.

Network Topology

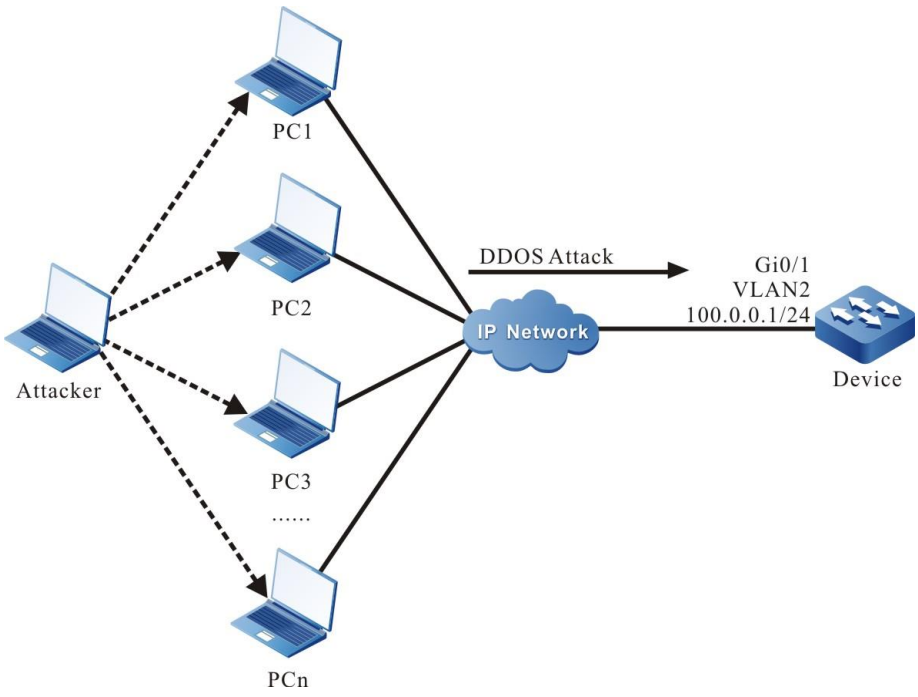


Figure 273 Networking of configuring scan attack detection

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. It is required that the PC can access IP Network via Device (omitted).

Step 3: Configure the attack defense policy a on Device, and configure the scan attack detection function in the policy. The scanning level is high.

```
Device(config)#attack-defense policy a
Device(config-anti-policy-a)#detect scan level high action blacklist
Device(config-anti-policy-a)#exit
```

#On Device, globally apply the attack defense policy a.

```
Device(config)#attack-defense global apply policy a
```

#On Device, open the scan attack log switch.

```
Device(config)#attack-defense action logging scan
```

Step 3: Check the result:

#On Device, view the current applied attack defense policy.

```
Device#show attack-defense applied policy
attack-defense policy a
 detect scan level high action blacklist
```

#When an attacker initiates a scanning attack on Device, view the scanning attack log output on Device.

```
%ANTIATTACK-SCAN_PORT_ATTACK-4: vlan2 detect port scan attack.
%ANTIATTACK-SCAN_PORT_ATTACK-4:Detect 100.0.0.2 is attacking the system.
%ANTIATTACK-SCAN_IP_ATTACK-4: vlan2 detect ip scan attack.
```

#On Device, view the IP scan entry.

```
Device#show attack-defense scan ip-scan
   IP Scan Statistic :
     sip              dip-count          interface
     ------------------------------------------------------------


     100.0.0.3          4            vlan2
     100.0.0.4          4            vlan2
     100.0.0.5          4            vlan2
     100.0.0.6          4            vlan2
     100.0.0.3          4            gigabitethernet0/1
     100.0.0.4          4            gigabitethernet0/1
     100.0.0.5          4            gigabitethernet0/1
     100.0.0.6          4            gigabitethernet0/1
```

#On Device, view the Port scan entry.

```
Device#show attack-defense scan port-scan
   Port Scan Statistic :
     sip              dip              dport-count       interface
     ------------------------------------------------------------------------------
--
     100.0.0.3          101.0.0.1          1             vlan2
     100.0.0.3          101.0.0.2          1             vlan2
     100.0.0.3          101.0.0.3          1             vlan2
```

```
100.0.0.3          101.0.0.4          1          vlan2
     100.0.0.4          101.0.0.5          1          vlan2
100.0.0.4          101.0.0.6          1          vlan2
     100.0.0.4          101.0.0.7          1          vlan2
100.0.0.4          101.0.0.8          1          vlan2
100.0.0.5          101.0.0.9          1          vlan2
100.0.0.5          101.0.0.10         1          vlan2
     100.0.0.5          101.0.0.11         1          vlan2
100.0.0.5          101.0.0.12         1          vlan2
     100.0.0.6          101.0.0.13         1          vlan2
100.0.0.6          101.0.0.14         1          vlan2
     100.0.0.6          101.0.0.15         1          vlan2
100.0.0.6          101.0.0.16         1          vlan2
100.0.0.3          101.0.0.1          1          gigabitethernet0/1
100.0.0.3          101.0.0.2          1          gigabitethernet0/1
     100.0.0.3          101.0.0.3          1          gigabitethernet0/1
100.0.0.3          101.0.0.4          1          gigabitethernet0/1
     100.0.0.4          101.0.0.5          1          gigabitethernet0/1
100.0.0.4          101.0.0.6          1          gigabitethernet0/1
     100.0.0.4          101.0.0.7          1          gigabitethernet0/1
100.0.0.4          101.0.0.8          1          gigabitethernet0/1
100.0.0.5          101.0.0.9          1          gigabitethernet0/1
100.0.0.5          101.0.0.10         1          gigabitethernet0/1
     100.0.0.5          101.0.0.11         1          gigabitethernet0/1
100.0.0.5          101.0.0.12         1          gigabitethernet0/1
     100.0.0.6          101.0.0.13         1          gigabitethernet0/1
100.0.0.6          101.0.0.14         1          gigabitethernet0/1
     100.0.0.6          101.0.0.15         1          gigabitethernet0/1
100.0.0.6          101.0.0.16         1          gigabitethernet0/1
```

#On Device, view the dynamic blacklist entry generated by scanning.

```
Device#show blacklist ip
Blacklist Info:
IpAddr,          CreateTime,          Agetime
-----------------------------------------------------------------------
100.0.0.2        ,  Mon May 04 17:36:45 2020     , 94
```

Note

- The flood attack and scan attack detection functions are effective for both local and forwarded packets on the router.

- Flood attack tracing or scanning attack will add to the dynamic blacklist after identifying the specific attack source. The aging time is 2min. Before the blacklist aging, all packets of the attack source will be intercepted.

9.16.3.4 Configure URPF Strict Mode

Network Requirements

- PC accesses IP Network through Device.
- Configure URPF strict mode on Device.
- The PC simulates the attacker to send an illegal packet with pseudo source address to access IP Network, and the URPF function of Device discards this packet.

Network Topology

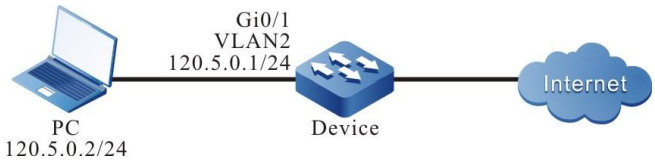


Figure 274 Networking of configuring URPF strict mode

Configuration Steps

Step 1: Configure VLAN and add the port to the corresponding VLAN. (omitted)

Step 2: Configure the IP address and route of each interface. It is required that the PC can access IP Network through Device. (omitted)

Step 3: Configure the URPF strict mode.

#Enable the URPF function on Device and configure the URPF strict mode on the interface vlan2.

```
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:

#PC1 accesses IP Network through Device, and the source address is 120.5.0.2.

There is a route to 120.5.0.2 on Device, and the route out interface is VLAN2. The out interface of the route to the source address and the receiving interface of the packet are the same interface VLAN2. Through URPF strict check, the packet is forwarded by Device, and PC1 can access Internet.

#PC simulates an attacker to send an illegal packet with a pseudo source address and accesses IP Network through Device. The source address is 120.10.0.2.

There is no route to 120.10.0.2 on Device, URPF discards the packet, and PC cannot access IP Network.

9.16.3.5 Configure URPF Loose Mode

Network Requirements

- In the network environment, PC1 accesses PC2 through Device1, Device2 and Device3, and the response packet of PC2 reaches PC1 through Device3 and Device1.
- Configure the URPF loose mode.
- PC1 simulates an attacker to send an illegal packet with a pseudo source address to access PC2, and the URPF function of Device discards this packet.

Network Topology

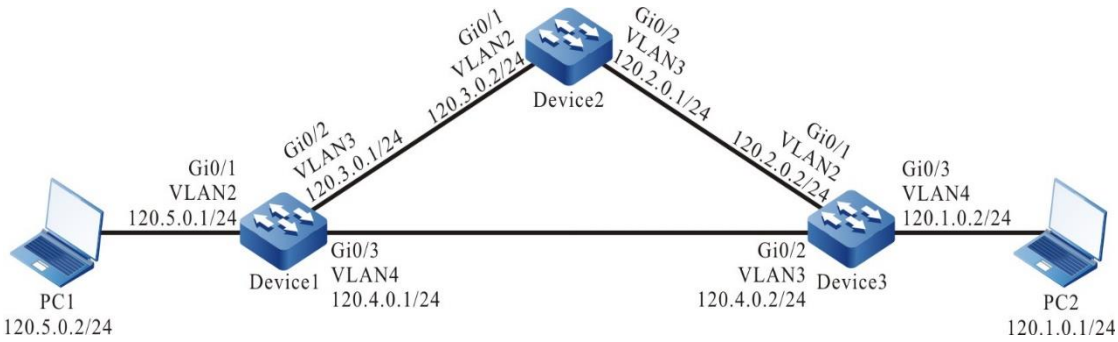


Figure 275 Networking of configuring the URPF loose mode

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 static route in the network so that PC1 accesses PC2 through Device1, Device2 and Device3. The response packet of PC2 reaches PC1 through Device3 and Device1.

#Configure the static route of Device1, Device2 and Device3, and construct the network environment in the 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
```

#View the route tables of Device1, Device2, and 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-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 the URPF loose mode on Device3.

#Enable the URPF function on Device3 and configure the URPF loose mode on interface vlan2.

```
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

The ping request packet of PC1 reaches PC2 through Device1, Device2 and Device3; The ping response packet of PC2 reaches PC1 through Device3 and Device1.

#PC1 accesses PC2, and the source address is 120.5.0.2.

There is a route to 120.5.0.2 on Device3, and the out interface of the route is vlan3. Although the out interface vlan3 of the route to the source address and the receiving interface vlan2 of the packet are not the same interface, through the URPF loose mode function check, the packet is forwarded by Device3, PC1 can access PC2, and the response message of PC2 reaches PC1 through Device3 and Device1.

#PC1 simulates an attacker to send an illegal packet with a pseudo source address to access PC2. The source address is 120.10.0.2.

There is no route to 120.10.0.2 on Devic3, URPF discards the packet, and PC1 cannot access PC2.

Note

- The packet discarding generated by the detection will not generate the log and statistics information.
- The difference between the strict and loose modes of URPF is: in the loose mode, URPF will search the route table for the source IP address of the received packet. If a route is found, the message is allowed to pass through; In the strict mode, the packet is allowed to pass only when the route is found and the outgoing interface is the same as the receiving interface of the packet.
- The strict mode is generally applied, and the loose mode is applied to the network environment with "inconsistent back and forth paths" in similar cases.

9.17 ARP Security

9.17.1 Overview

ARP (Address Resolution Protocol) security is a security feature against ARP attacks. It ensures the security of network devices through a series of measures such as restriction and inspection of ARP packet processing. ARP security features can not only prevent attacks against ARP protocol, but also prevent network segment scan attacks and other attacks based on the ARP protocol.

9.17.2 ARP Security Function Configuration

Table 1262 ARP security function configuration list

Configuration tasks	
Configure the ARP security function	Configure intercepting ARP speed limit, ARP speed limit with fixed source MAC address, ARP speed limit with fixed source IP address, and ARP source address suppression attack packet detection

Note: The intercepted packets configured by the software on the switch is only valid for the packet to the local machine.

9.17.2.1 Configure ARP Speed Restriction Function

The ARP speed limit function is mainly used to protect the server from the impact of large traffic ARP packets. ARP speed limit detection can be configured globally or on the interface, or applied globally. When ARP speed limit detection is configured globally, ARP speed limit detection is performed for ingress ARP packets; When the interface is configured with ARP speed limit detection, ARP speed limit detection is performed on the ingress packets of the interface configured with ARP speed limit function; When ARP speed limit detection is applied globally, enable the ARP speed limit detection function on the interface. When it is detected that the ingress packet rate on the global or interface continues to exceed the specified trigger threshold, it is

considered that the global or interface has been attacked by ARP speed limit, it will enter the attack prevention state and start the corresponding prevention policy according to the configuration. The default behavior of ARP speed limit function is to discard the packet, which is not configurable, and the output log alarm can be configured. When the device detects that this type of packet traffic is lower than the threshold for 5 seconds, release the attack state and stop executing attack prevention measures.

Configuration Conditions

- Configure ARP speed limit detection globally to enable global ARP speed limit detection.
- Configure ARP speed limit detection on the specified interface to enable ARP speed limit detection on the specified interface.
- Apply ARP speed limit detection globally to enable ARP speed limit detection on the interface.

Configure Interrupting Global ARP Speed Limit Attack Packet

When the packets detected by ARP speed limit exceed the threshold in the global mode, adopt the corresponding preventive measures.

Table 1263 Configure global ARP speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure global ARP speed limit	arp speed-limit threshold *threshold-value*	Mandatory By default, do not enable the global ARP speed limit detection.

Configure Interrupting Interface ARP Speed Limit Attack Packet

When the packets detected by ARP speed limit exceed the threshold in the interface mode, adopt the corresponding preventive measures.

It can also be configured in the switch port.

Table 1264 Configure the interface ARP speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the interface ARP speed limit	arp speed-limit threshold *threshold-value*	Mandatory By default, do not enable the interface ARP speed limit detection.

Configure Interrupting ARP Speed Limit Attack Packet in L2 VLAN

When the packets detected by ARP speed limit exceed the threshold in the L2 VLAN mode, adopt the corresponding preventive measures.

Table 1265 Configure ARP speed limit in L2 VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	Mandatory
Configure the ARP speed limit detection in the L2 VLAN	arp speed-limit threshold *threshold-value*	Mandatory By default, do not configure the ARP speed limit detection in the L2 VLAN.

Configure Globally Applying ARP Speed Limit Attack Detection

When configuring ARP speed limit detection for global application, it takes effect under each interface. If the global application and the configuration under the interface

exist at the same time, the configuration under the interface takes precedence.

Table 1266 Configure globally applying ARP speed limit attack detection

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure globally applying ARP speed limit attack detection	**arp global apply speed-limit threshold** *threshold-value*	Mandatory By default, do not configure globally applying ARP speed limit attack detection.

Configure ARP Security Attack Prevention Log Record

When the device detects the ARP packet attack, adopt the prevention policy and make the log record.

Table 1267 Configure the ARP security attack log output

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the ARP security attack log output	attack-defense action logging flood	Mandatory By default, do not enable the ARP security attack log.

9.17.2.2 Configure ARP Source MAC Address Speed Limit Function

The ARP source MAC address speed limit function is mainly used to protect the server from the impact of large traffic ARP packets. ARP source MAC address speed limit detection can be configured globally or on the interface, or ARP source MAC address speed limit detection can be applied globally. When the ARP source MAC address speed limit detection is configured globally, perform the ARP source MAC address speed limit detection for the ingress ARP packets; When the ARP source MAC address speed limit detection is configured on the interface, perform the ARP source MAC address speed limit detection for the incoming packets of the interface configured

with the ARP source MAC address speed limit function; When the ARP source MAC address speed limit detection is applied globally, enable the ARP source MAC address speed limit detection function on the interface. When it is detected that the packet rate from the same source address in the incoming direction of the global or interface continues to exceed the specified trigger threshold, it is considered that the global or interface has been attacked by the ARP source address speed limit, it will enter the attack prevention state, and start the corresponding prevention policy according to the configuration (output the alarm log, discard the packet, and add the attack source to the dynamic blacklist). When the device detects that the packet traffic of this type is lower than the threshold or the generated dynamic blacklist is aged for 5 seconds, release the attack state and stop executing attack prevention measures.

Configuration Conditions

- Configure ARP source MAC address speed limit detection globally to enable global ARP source MAC speed limit detection.
- Configure ARP source MAC address speed limit detection on the specified interface to enable ARP source MAC address speed limit detection on the specified interface.
- Apply ARP source MAC address speed limit detection globally to enable ARP source MAC address speed limit detection on the interface.

Configure Interrupting Global ARP Source MAC Address Speed Limit Attack Packet

When the packets detected by ARP source MAC address speed limit exceed the threshold in the global mode, adopt the corresponding preventive measures.

Table 1268 Configure global ARP source MAC address speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure global ARP	arp speed-limit source-mac [threshold	Mandatory

source MAC address speed limit	*threshold-value*] [action { drop | blacklist }*]	By default, do not configure global ARP source MAC address speed limit.

Configure Interrupting Interface ARP Source MAC Address Speed Limit Attack Packet

When the packets detected by ARP source MAC address speed limit exceed the threshold in the interface mode, adopt the corresponding preventive measures.

It can also be configured in the switch port.

Table 1269 Configure the interface ARP source MAC address speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the interface ARP source MAC address speed limit	arp speed-limit source-mac [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure the interface ARP source MAC address speed limit.

Configure Interrupting ARP Source MAC Address Speed Limit Attack Packet in L2 VLAN

When the packets detected by ARP source MAC address speed limit exceed the threshold in the L2 VLAN mode, adopt the corresponding preventive measures.

Table 1270 Configure ARP source MAC address speed limit in L2 VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Enter the VLAN configuration mode	vlan *vlan-id*	Mandatory
Configure ARP source MAC address speed limit detection in L2 VLAN	arp speed-limit source-mac [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not Configure ARP source MAC address speed limit detection in L2 VLAN.

Configure Globally Applying ARP Source MAC Address Speed Limit Attack Detection

When configuring ARP source MAC address speed limit detection for global application, it takes effect under each interface. If the global application and the configuration under the interface exist at the same time, the configuration under the interface takes precedence.

Table 1271 Configure globally applying ARP source MAC address speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure globally applying ARP source MAC address speed limit	arp global apply speed-limit source-mac [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not Configure globally applying ARP source MAC address speed limit.

9.17.2.3 Configure ARP Source IP Address Speed Limit Function

The ARP source IP address speed limit function is mainly used to protect the server from the impact of large traffic ARP packets. ARP source IP address speed limit detection can be configured globally or on the interface, or ARP source IP address speed limit detection can be applied globally. When the ARP source IP address speed limit detection is configured globally, perform the ARP source IP address speed limit detection for the ingress ARP packets; When the ARP source IP address speed limit

detection is configured on the interface, perform the ARP source IP address speed limit detection for the incoming packets of the interface configured with the ARP source IP address speed limit function; When the ARP source IP address speed limit detection is applied globally, enable the ARP source IP address speed limit detection function on the interface. When it is detected that the packet rate from the same source address in the incoming direction of the global or interface continues to exceed the specified trigger threshold, it is considered that the global or interface has been attacked by the ARP source address speed limit, it will enter the attack prevention state, and start the corresponding prevention policy according to the configuration (output the alarm log, discard the packet, and add the attack source to the dynamic blacklist). When the device detects that the packet traffic of this type is lower than the threshold or the generated dynamic blacklist is aged for 5 seconds, release the attack state and stop executing attack prevention measures.

Configuration Conditions

- Configure ARP source IP address speed limit detection globally to enable global ARP source IP speed limit detection.
- Configure ARP source IP address speed limit detection on the specified interface to enable ARP source IP address speed limit detection on the specified interface.
- Apply ARP source IP address speed limit detection globally to enable ARP source IP address speed limit detection on the interface.

Configure Interrupting Global ARP Source IP Address Speed Limit Attack Packet

When the packets detected by ARP source IP address speed limit exceed the threshold in the global mode, adopt the corresponding preventive measures.

Table 1272 Configure global ARP source IP address speed limit

Step	Command	Description
Enter the global configuration	configure terminal	-

mode		
Configure the interface ARP source IP address speed limit detection	arp speed-limit source-ip [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure the interface ARP source MAC address speed limit detection.

Configure Interrupting Interface ARP Source IP Address Speed Limit Attack Packet

When the packets detected by ARP source IP address speed limit exceed the threshold in the interface mode, adopt the corresponding preventive measures.

It can also be configured in the switch port.

Table 1273 Configure the interface ARP source IP address speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the interface ARP source IP address speed limit	arp speed-limit source-ip [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure the interface ARP source IP address speed limit.

Configure Interrupting ARP Source IP Address Speed Limit Attack Packet in L2 VLAN

When the packet detected by ARP source IP address speed limit exceeds the threshold in the L2 VLAN mode, adopt the corresponding preventive measures.

Table 1274 Configure ARP source IP address speed limit in L2 VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Enter the VLAN configuration mode	vlan *vlan-id*	Mandatory
Configure ARP source IP address speed limit detection in L2 VLAN	arp speed-limit source-ip [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure ARP source IP address speed limit detection in L2 VLAN.

Configure Globally Applying ARP Source IP Address Speed Limit Attack Detection

When configuring ARP source IP address speed limit detection for global application, it takes effect under each interface. If the global application and the configuration under the interface exist at the same time, the configuration under the interface takes precedence.

Table 1275 Configure globally applying ARP source IP address speed limit

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure globally applying ARP source IP address speed limit	arp global apply speed-ip source-mac [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure globally applying ARP source IP address speed limit detection.

9.17.2.4 Configure ARP Source Address Suppression Function

The ARP source address suppression function is mainly used to protect the server from the impact of a large traffic of the IP packets whose destination IP addresses cannot be resolved. ARP source address suppression detection can be configured globally or on the interface, or ARP source address suppression detection can be

applied globally. When the source ARP address suppression detection is configured globally, perform the ARP source address suppression detection for the ingress IP packet; When the interface is configured with ARP source address suppression detection, perform ARP source address suppression detection on the ingress packet of the interface configured with ARP source address suppression function; When ARP source address suppression detection is applied globally, enable the ARP source address suppression detection function on the interface. When it is detected that the rate of the ingress IP packets from the same source IP address on the global or interface and whose destination IP addresses cannot be resolved continuously exceeds the specified trigger threshold, it is considered that the global or interface has been attacked by ARP source address suppression, and it enters the attack prevention state, and start corresponding prevention policies according to the configuration (output alarm log, discard the packet, add attack source to dynamic blacklist). When the device detects that the packet traffic of this type is lower than the threshold or the generated dynamic blacklist is aged for 5 seconds, release the attack state and stop executing attack prevention measures.

Configuration Conditions

- Configure ARP source address suppression detection globally to enable global ARP source address suppression detection.
- Configure ARP source address suppression detection on the specified interface to enable ARP source address suppression detection on the specified interface.
- Apply ARP source address suppression detection globally to enable ARP source address suppression detection on the interface.

Configure Interrupting Global ARP Source Suppression Attack Packet

When the packets detected by ARP source address suppression exceed the threshold in the global mode, adopt the corresponding preventive measures.

Table 1276 Configure global ARP source address suppression

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure global ARP source address suppression detection	arp source-suppression [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure global ARP source address suppression detection.

Configure Interrupting Interface ARP Source Suppression Attack Packet

When the packets detected by ARP source address suppression in the interface exceed the threshold, adopt the corresponding preventive measures.

It can also be configured in the switch port.

Table 1277 Configure interface ARP source address suppression

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the interface ARP source address suppression detection	arp source-suppression [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure the interface ARP source address suppression detection.

Configure Interrupting ARP Source Address Suppression Attack Packet in L2 VLAN

When the packets detected by ARP source address suppression exceed the threshold in the L2 VLAN mode, adopt the corresponding preventive measures.

Table 1278 Configure ARP source address suppression in L2 VLAN

Step	Command	Description

Enter the global configuration mode	configure terminal	-
Enter the VLAN configuration mode	vlan *vlan-id*	Mandatory
Configure ARP source address suppression detection in L2 VLAN	arp source-suppression [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure ARP source address suppression detection in L2 VLAN.

Configure Globally Applying ARP Source Address Suppression Attack

When configuring ARP source address suppression detection for global application, it takes effect under each interface. If the global application and the configuration under the interface exist at the same time, the configuration under the interface takes precedence.

Table 1279 Configure globally applying ARP source address suppression

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure globally applying ARP source address suppression	arp global apply source-suppression [threshold *threshold-value*] [action { drop | blacklist }*]	Mandatory By default, do not configure globally applying ARP source address suppression.

9.17.2.5 ARP Security Monitoring and Maintaining

Table 1280 ARP security monitoring and maintaining

Command	Description
clear arp source-suppression statistics [member *member-ID*] { interface [*interface-name*] | vlan [*vlan-id*] }	Clear the ARP source address suppression statistics information on the interface
clear arp source-suppression statistics global [member *member-ID*]	Clear global ARP source address suppression statistics information

clear arp speed-limit [source-ip | source-mac] statistics [member *member-ID* { interface [*interface-name*] | vlan [*vlan-id*] }	Clear the ARP speed limit statistics information
clear arp speed-limit [source-ip | source-mac] statistics global [member *member-ID*]	Clear global ARP speed limit statistics information
show arp source-suppression statistics [member *member-ID*] { interface [*interface-name*] | vlan [*vlan-id*] }	Display the ARP source address suppression statistics information on the interface
show arp source-suppression statistics global [member *member-ID*]	Display the global ARP source address suppression statistics information
show arp speed-limit [source-ip | source-mac] statistics [member *member-ID*] { interface [*interface-name*] | vlan [*vlan-id*] }	Display the ARP speed limit statistics information on the interface
show arp speed-limit { source-ip | source-mac } statistics global [member *member-ID*]	Display the global ARP speed limit statistics information

9.17.3 ARP Security Typical Configuration Example

9.17.3.1 Configure ARP Speed Limit Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.
- Device configures ARP speed limit detection function. When ARP attack packet is detected, output alarm log and discard attack packet.

Network Topology

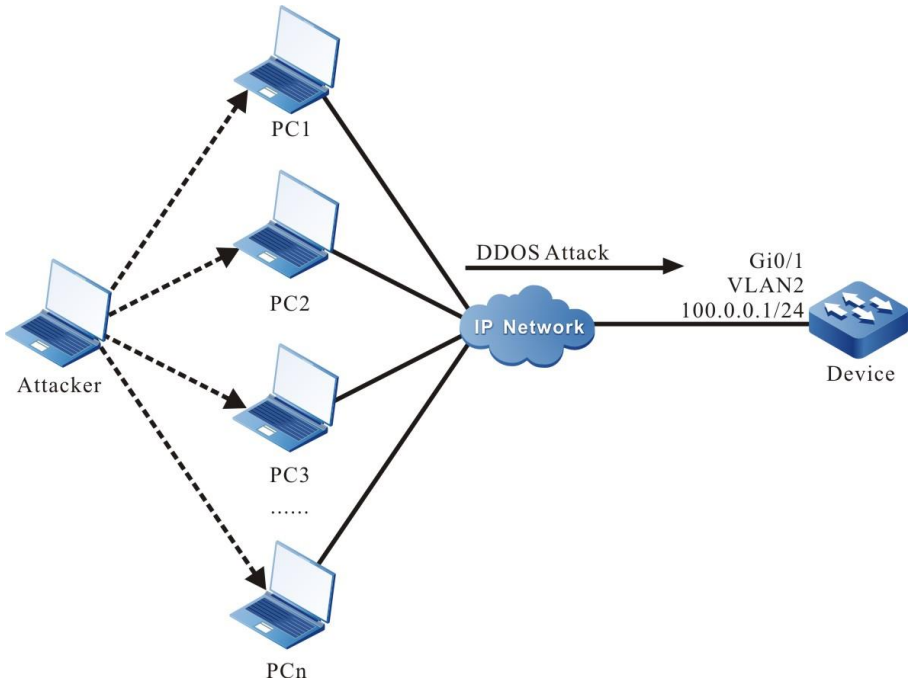


Figure 276 Networking of configuring ARP speed limit detection

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 ARP speed limit detection function on Device port gigabitethernet0/1.

```
Device(config)#interface gigabitethernet0/1
Device(config-if-gigabitethernet0/1)#arp speed-limit
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 4: Check the result.

#On Device, view the current ARP security configuration.

```
Device#show running-config interface gigabitethernet 0/1
Building Configuration...
interface gigabitethernet0/1
```

```
switchport access vlan 2
arp speed-limit
exit
```

#When an attacker sends an ARP packet to Device and the number of ARP packets received by Device port gigabitethernet0/1 exceeds 100 per unit time, it recognizes the ARP packet speed limit attack, outputs the ARP speed limit attack alarm log, and discards the excessive ARP packets.

```
%ANTIATTACK-ARP_ATTACK-4:interface gigabitethernet0/1 detect attack, type speed-limit.
```

#On Device, view the ARP speed limit statistics information.

```
Device#show arp speed-limit statistics interface gigabitethernet0/1
  Speed-limit Info:
  Interface                LastRecvTime              DropCount  Token
  ------------------------------------------------------------------------------
-------------
  gigabitethernet0/1       Wed Mar 23 07:23:53 2021      250       0
```

9.17.3.2 Configure ARP Source MAC Address Speed Limit Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.
- Device configures the ARP source MAC address speed limit detection function. When an ARP speed limit attack with a fixed source MAC address is detected, output the alarm log, and add the identified attack source MAC address to the blacklist. Discard the attack packet before the blacklist table entry is generated.

Network Topology

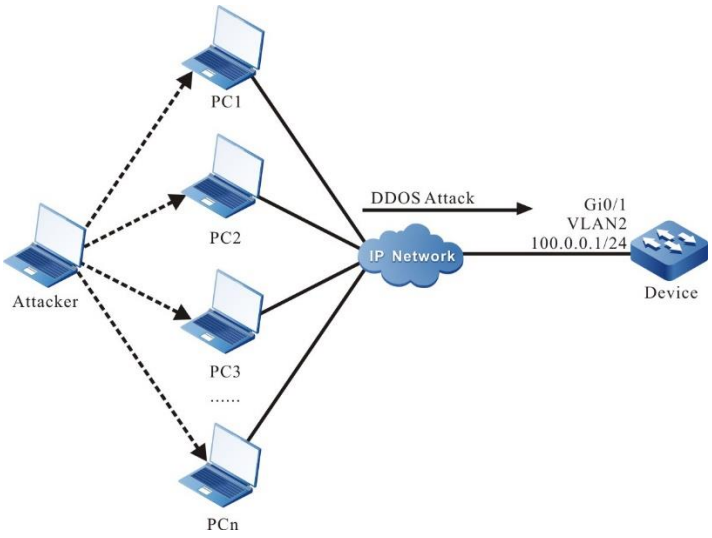


Figure 277 Networking of configuring ARP source MAC address speed limit

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 ARP source MAC address speed limit detection function on Device port gigabitethernet0/1.

```
Device(config)#interface gigabitethernet0/1
Device(config-if-gigabitethernet0/1)#arp speed-limit source-mac action blacklist drop
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 4: Check the result.

#On Device, view the current ARP security configuration.

```
Device#show running-config interface gigabitethernet 0/1
Building Configuration...
interface gigabitethernet0/1
switchport access vlan 2
 arp speed-limit source-mac action drop blacklist
 exit
```

#When an attacker sends an ARP packet to Device and the number of the ARP packets with fixed source MAC addresses received by Device port gigabitethernet0/1 exceeds 100 per unit time, it identifies the ARP source MAC address speed limit attack, outputs the ARP speed limit attack alarm log containing the attack source MAC information, adds the identified attack source MAC address to the blacklist, and discards the attack packet before the blacklist table entry is generated.

```
%ANTIATTACK-ARP_MAC_ATTACK-4:interface gigabitethernet0/1 detect attack, type speed-limit, mac 0010.9400.0002.
```

#On Device, view the ARP source MAC address speed limit statistics information.

```
Device#show arp speed-limit source-mac statistics interface gigabitethernet0/1
  Speed-limit Info:
  MAC              Interface              LastRecvTime              DropCount  Token
  ------------------------------------------------------------------------------------
  0010.9400.0002   gigabitethernet0/1     Wed Mar 23 07:28:19 2021  1          0
```

#View the dynamic blacklist items generated by traceability on Device.

```
Device#show blacklist dynamic mac
  Blacklist Info:
  Mac              CreateTime              Agetime
  ------------------------------------------------------------------
  0010.9400.0002   Wed Mar 23 07:28:20 2021  114
```

9.17.3.3 Configure ARP Source IP Address Speed Limit Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.
- Device configures the ARP source IP address speed limit detection function. When an ARP speed limit attack with a fixed source IP address is detected, output the alarm log, add the identified attack source IP address to the blacklist, and discard the attack packet before the blacklist table entry is generated.

Network Topology

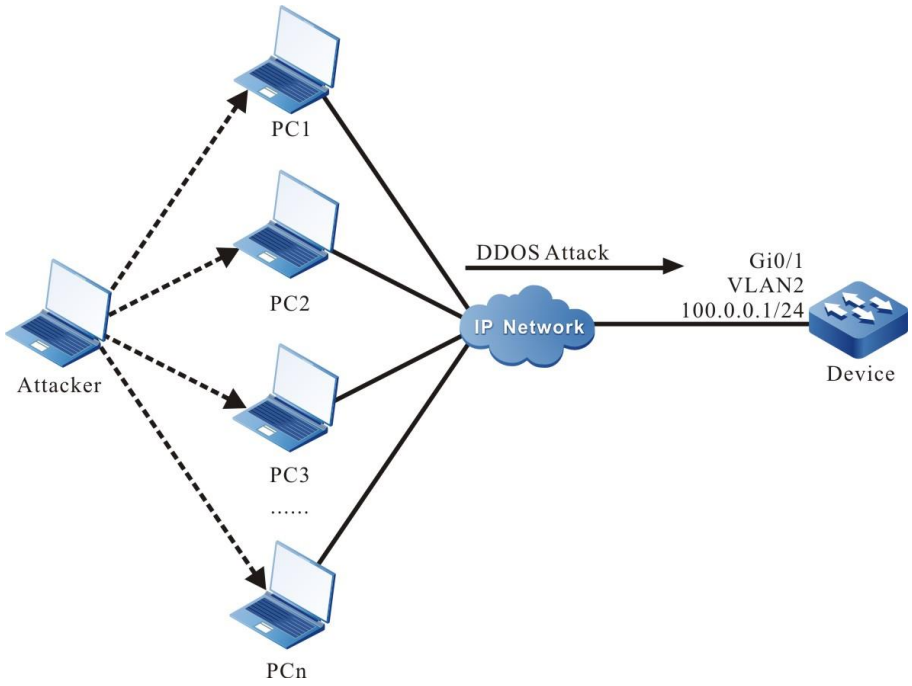


Figure 278 Networking of configuring ARP source IP address speed limit

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 ARP source IP address speed limit detection function on Device port gigabitethernet0/1.

```
Device(config)#interface gigabitethernet0/1
Device(config-if-gigabitethernet0/1)#arp speed-limit source-ip action blacklist drop
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 4: Check the result.

#On Device, view the current ARP security configuration.

```
Device#show running-config interface gigabitethernet 0/1
Building Configuration...
interface gigabitethernet0/1
```

```
switchport access vlan 2
 arp speed-limit source-ip action drop blacklist
 exit
```

#When an attacker sends an ARP packet to Device and the number of the ARP packets with fixed source IP addresses received by Device port gigabitethernet0/1 exceeds 100 per unit time, it identifies the ARP source IP address speed limit attack, outputs the ARP speed limit attack alarm log containing the attack source IP information, adds the identified attack source IP address to the blacklist, and discards the attack packet before the blacklist table entry is generated.

```
%ANTIATTACK-ARP_IP_ATTACK-4:interface gigabitethernet0/1 detect attack, type speed-limit, ipaddr 100.0.0.2.
%ANTIATTACK-ARP_IP_ATTACK-4:interface gigabitethernet0/1 detect attack, type speed-limit, ipaddr 100.0.0.3.
```

#On Device, view the ARP source IP address speed limit statistics information.

```
Device#show arp speed-limit source-ip statistics interface gigabitethernet0/1
  Speed-limit Info:
  IpAddr          Interface              LastRecvTime              DropCount   Token
  ------------------------------------------------------------------------------------
------------------------------------
      100.0.0.2       gigabitethernet0/1     Wed Mar 23 07:32:51 2021    1       0
      100.0.0.3       gigabitethernet0/1     Wed Mar 23 07:32:51 2021    1       0
```

#View the dynamic blacklist items generated by traceability on Device

```
Device#show blacklist dynamic ip
  Blacklist Info:
  IpAddr          CreateTime             Agetime
  ------------------------------------------------------------------
  100.0.0.2       Wed Mar 23 07:32:51 2021    116
  100.0.0.3       Wed Mar 23 07:32:51 2021    116
```

9.17.3.4 Configure ARP Source Address Suppression Detection

Network Requirements

- Device accesses the IP network through gigabitethernet0/1.
- Device configures ARP source address suppression detection function. When ARP source address suppression attack packet is detected, it outputs alarm log and discards attack packet.

Network Topology

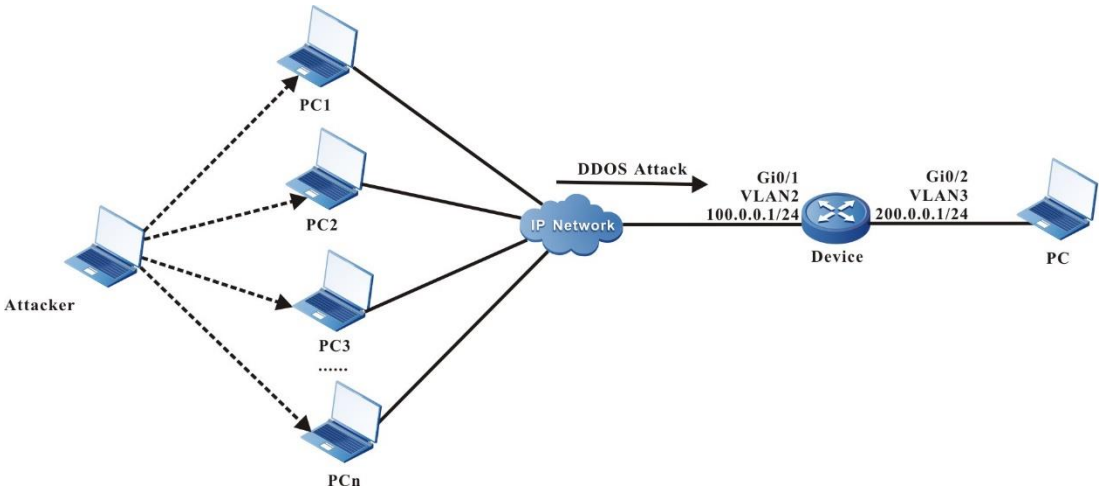


Figure 279 Networking of configuring ARP source address suppression detection

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 (omitted).

Step 3: On Device port gigabitethernet0/1, configure the ARP source address suppression detection function.

```
Device(config)#interface gigabitethernet0/1
Device(config-if-gigabitethernet0/1)#arp source-suppression action drop
Device(config-if-gigabitethernet0/1)#exit
```

#On Device, open the flood attack log switch.

```
Device(config)#attack-defense action logging flood
```

Step 4: Check the result.

#On Device, view the current ARP security configuration.

```
Device#show running-config interface gigabitethernet 0/1
Building Configuration...
interface gigabitethernet0/1
switchport access vlan 2
 arp source-suppression
 exit
```

#The attacker sends an IP packet to the device whose destination IP address cannot

be resolved. When the number of IP packets with the same source IP address and the destination IP address cannot be resolved exceeds 100, identify the ARP source address suppression attack, output the ARP source address suppression attack alarm log containing the attack source IP information, and discard the attack packet.

```
%ANTIATTACK-ARP_IP_ATTACK-4:interface gigabitethernet0/1 detect attack, type source-suppression, ipaddr 192.85.1.2.
```

#On Device, view the ARP source address suppression statistics information.

```
Device#show arp source-suppression statistics interface gigabitethernet0/1
  Suppression Info:
  IpAddr          Interface              LastRecvTime              DropCount  Token
  ------------------------------------------------------------------------------------
-------------------------------------
  192.85.1.2      gigabitethernet0/1     Wed Mar 23 07:44:47 2021  300        0
```

9.18 AARF

9.18.1 AARF Introduction

AARF is short for Anti Attack Resilient Framework.

9.18.2 AARF Overview

In the network environment, the switches are often attacked by malicious packets (ARP, ICMP, etc.). These malicious attacks impose heavy burdens on the switch system and make the system unable to continue running. Usually, a large number of packets will consume the CPU utilization, memory, table entries or other resources of the switch. As a result, the other normal protocol packets and management packets cannot be processed by the system, or even the whole network cannot run.

AARF can effectively identify and prevent the switch from being affected by these attacks. It can ensure the normal operation of the system and protect the CPU from excessive load when the switch is attacked, so that the whole network can run normally.

9.18.3 AARF Principles

Generally speaking, the principle of protocol packet anti-attack is to count the packets sent to CPU, calculate the rate of sending them, and then compare with the set

attack threshold. If the rate reaches the attack threshold, it is considered that the protocol packet has attack behavior, and then, perform some restrictions for the host with the attack behavior, such as CPU discarding, speed limit, and filtering, so as to protect the CPU.

In fact, from the view of implementation, different protocol packet anti-attack functions have the same implementation method for packet statistics, identification, attack policy application, and so on. We abstract the same processing, build a framework, and form AARF. AARF is used to implement some common processing mechanisms of the anti-attack module, so as to enhance the scalability of the anti-attack module and reduce the workload of developing new protocol anti-attack module.

Currently, AARF supports the ARP guard (arp-guard).

9.18.4 ARP Anti-Attack

ARP guard (arp-guard) is a real-time monitoring function for the ARP packets to the CPU, preventing a large number of ARP packets from impacting the CPU and improving the security of the device.

ARP guard includes host-based ARP guard, port-based ARP guard and ARP scanning identification.

Host-based ARP guard counts the received ARP packets, and then, compares the statistics value with the set threshold. If exceeding the threshold, it is identified as speeding or attack. The statistics and identification are based on the source IP address/VLAN ID/port and link-layer source MAC address/VLAN ID/port.

Port-based ARP guard counts the number of the ARP packets received by the port without host attack. If exceeding the threshold set by the port, it is identified as speeding or attack. Port statistics does not include the ARP packets that have been identified as host attacks (host table entries are generated and attack protection policies are applied).

ARP scanning identification can identify two kinds of ARP scanning: the ARP

scanning with fixed source MAC address and variable source IP, and the ARP scanning with fixed source MAC and source IP and variable destination IP.

9.18.4.1 ARP Guard Function Configuration

Table 1281 ARP guard function configuration list

Configuration tasks	
Configure the basic functions of the ARP guard	Enable the global ARP guard function
	Enable the ARP guard function on the port
Configure the monitor policy of the ARP guard	Configure the global monitor policy
	Configure the monitor policy on the port

9.18.4.2 Configure the Basic Functions of ARP Guard

Port-based ARP guard function can take effect only after the global ARP guard function is enabled.

Configuration Condition

None

Enable Global ARP Guard Function

Table 1282 Enable the global ARP guard function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the AARF configuration mode	aarf	-
Enable the global ARP guard function	arp-guard enable	Mandatory By default, do not enable the ARP guard function globally.

Enable Port ARP Guard Function

Table 1283 Enable the port ARP guard function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 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	interface link-aggregation *link-aggregation-id*	
Enable the port ARP guard function	aarf arp-guard enable	Mandatory By default, do not enable the ARP guard function on the port.

9.18.4.3 Configure the Monitor Policy of ARP Guard

Configuration Condition

None

Configure the Monitor Policy of Global ARP Guard

Table 1284 Configure the monitor policy of the global ARP guard function

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the AARF configuration mode	aarf	-
Configure the monitor policy of the global ARP guard	arp-guard policy { filter | monitor | punish macbased}	By default, the monitor policy of the global ARP guard is monitor.

Configure the Monitor Policy of Port ARP Guard

Table 1285 Configure the monitor policy of the port ARP guard

Step	Command	Description
Enter global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 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	interface link-aggregation *link-aggregation-id*	
Configure the monitor policy of the port ARP guard	aarf arp-guard policy { filter | monitor | punish macbased}	By default, the monitor policy of the port ARP guard is not configured, and the monitor policy of the global ARP guard takes effect.

The **aarf arp-guard policy filter** command is a protection policy of filtering the hosts applied to the host or port with ARP attack under the port. After configuring the filtering policy, generate the attack alarm after detecting the host with ARP over-speed or attack behavior under the port, and if the speed of the host sending ARP packets is between the speed threshold and attack threshold, the speed of the ARP packets to the CPU will be limited to the speed threshold. The ARP packets in the forwarding direction will be forwarded at the sending speed of the host; if the speed of the host sending ARP packets exceeds the attack threshold, the ARP packets to the CPU will be dropped. If detecting that the port has the overspend or attack behavior (i.e., the total rate of the port receiving the ARP packets from all non-attack hosts is greater than or equal to the port speed threshold or attack threshold), generate the attack alarm. If the total rate of the port receiving the ARP packets from the non-attack hosts is between the port speed threshold and the port attack threshold, the total rate of the port receiving the ARP packets from the non-attack hosts limits the speed of the ARP packets to the

CPU by the port speed threshold, and the ARP packets to be forwarded are forwarded by the initial speed. If the total rate of the port receiving the ARP packets from non-attack hosts is greater than or equal to the port attack threshold, all ARP packets received by the port will be discarded in the forwarding direction and will not be sent to the CPU.

The **aarf arp-guard policy monitor** command is a protection policy of monitoring the host applied to the host or port with the ARP attack under the port. After configuring the monitoring policy, generate the attack alarm after detecting the host packet or port with ARP speeding or attack behavior is detected under the port, but the packet will be sent to the CPU at the rate of the speed limit threshold, and the ARP packet beyond the speed limit will be discarded by the CPU; the ARP packet to be forwarded will be forwarded at the initial rate.

The **aarf arp-guard policy punish macbased** command is a protection policy of punishing the speed limit applied to the MAC hosts with the ARP attacks under the port. After configuring the policy of punishing the speed limit, generate the attack alarm when detecting the MAC host packet with ARP speeding or attack behavior under the port. If the rate of the packets sent by the MAC host is between the speed-limit threshold and the attack threshold, the monitor policy will take effect. If the ARP packet rate is greater than or equal to the attack threshold, the MAC packets attacking the host will be sent to CPU and forwarded at half the rate of the MAC speed limit threshold. If the attack stops or the rate drops below the MAC speed limit threshold, remove the host protection policy when the aging period arrives. In addition, in this policy mode, both port and IP host use the monitor policy.

9.18.4.4 ARP Guard Monitoring and Maintaining

Table 1286 ARP guard monitoring and maintaining

Command	Description
show aarf arp-guard configure	Display the ARP guard configuration information
show aarf arp-guard hosts	Display the monitored host information
show aarf arp-guard ports	Display the monitored port information
show aarf arp-guard scan	Display the scanned host information

9.18.5 AARF ARP-Guard Typical Configuration Example

9.18.5.1 Configure the Basic Functions of AARF ARP-GUARD

Network Requirements

- PC1, PC2, and PCs are connected to IP Network via Device.
- PC1 sends the ARP packet to attack Device, Device enables AARF ARP-Guard, Device normally identifies the ARP overspeed, ARP attack, ARP MAC scan, ARP MAC-IP Scan, and the AARF ARP-Guard policy normally takes effect.

Network Topology

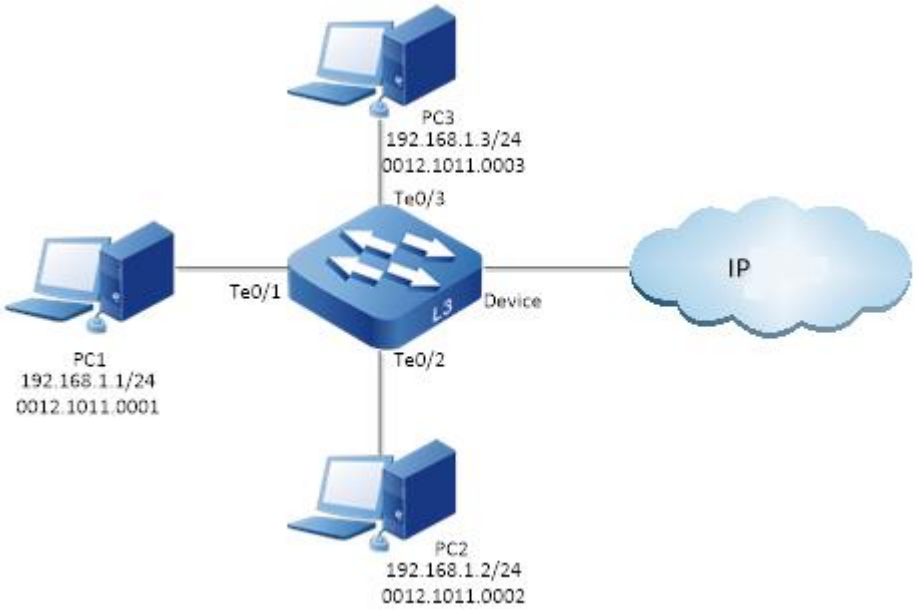


Figure 280 Networking for configuring the ARP guard function

Configuration Steps

Step 1: Configure the VLAN and port link type on Device.

#Create VLAN2.

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#Configure the link type of port tengigabitethernet0/1, tengigabitethernet0/2, and tengigabitethernet0/3 as Access, permitting the services of VLAN2 to pass.

```
Device(config)#interface tengigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
```

Step 2: Configure the gateways of PC1, PC2, and PC3 on Device.

#Configure VLAN interface 2 as the gateway of PC1, PC2, and PC3.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 192.168.1.254 24
```

Step 3: Enable AARF ARP-Guard on Device.

#Enable AARF ARP-Guard globally.

```
Device(config)#aarf
Device(config-aarf)#arp-guard enable
```

#Enable AARF ARP-Guard on port tengigabitethernet0/1, the related thresholds are the default values, and configure the policy as filter.

```
Device(config-if-tengigabitethernet0/1)# aarf arp-guard enable
Device(config-if-tengigabitethernet0/1)# aarf arp-guard policy filter
```

Step 4: Check the result.

#Query the AARF ARP-Guard configuration information.

```
Device#show aarf arp-guard configure  interface tengigabitethernet 0/1
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-interface.)
-------------------------------------------------------------------------------
----
Interface/Global  Status   Rate-limit   Attack-threshold   Scan-threshold  Attack-policy
-------------------------------------------------------------------------------
----
te0/1          Enabled   4/4/100      8/8/200           15              filter
```

#When the rate of PC1 sending the ARP Request packet for requesting Device Gateway IP address is larger than or equal to the host-based speed limit threshold 4pps and less than the host-based attack threshold 8pps, form the related table entries and output the log information. Device recognizes that the host-based ARP packet is overspeed.

```
Device#show aarf arp-guard hosts
-------------------------------------------------------------------------------
----
Interface               Vlan                    IP                  MAC
                    Action              Policy
-------------------------------------------------------------------------------
----
te0/1                   2                   192.168.1.1             -
        overspeed           monitor
te0/1                   2                   -                   0012.1011.0001
        overspeed           monitor
Total: 2 record(s).
```

#The output log is:

```
Dec 20 2016 03:45:28: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan
detected on interface te0/1.(TUE DEC 20 03:45:25 2016)
Dec 20 2016 03:45:28: %AARF-DETECTED-3:<arp-
guard>Host<IP=N/A,MAC=0012.1011.0001,interface= te0/1,VLAN=2> overspeed was
detected.(TUE DEC 20 03:45:25 2016)
Dec 20 2016 03:45:28: %AARF-DETECTED-3:<arp-
guard>Host<IP=192.168.1.1,MAC=N/A,interface= te0/1,VLAN=2> overspeed was detected.(TUE
DEC 20 03:45:25 2016)
```

#When the rate of PC1 sending the ARP Request packet for requesting Device Gateway IP address is larger than the host-based attack threshold 8pps, Device filters the ARP packet, forms the related table entries, and outputs the log information. Device identifies the host-based ARP packet attack.

```
Device#show aarf arp-guard hosts
-------------------------------------------------------------------------------
----
Interface               Vlan                    IP                  MAC
                    Action              Policy
-------------------------------------------------------------------------------
----
te0/1                   2                   192.168.1.1             -
        attack              filter
te0/1                   2                   -                   0012.1011.0001
        attack              filter
```

```
Total: 2 record(s).
```

#The output log is:

```
Dec 20 2016 04:30:33: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface te0/1.(TUE DEC 20 04:30:30 2016)
Dec 20 2016 04:30:33: %AARF-FILTER-3:<arp-guard>Host<IP=N/A,MAC=0012.1011.0001,interface=
te0/1,VLAN=2> attack was filter.(TUE DEC 20 04:30:30 2016)
Dec 20 2016 04:30:33: %AARF-FILTER-3:<arp-guard>Host<IP=192.168.1.2,MAC=N/A,interface=
te0/1,VLAN=2> attack was filter.(TUE DEC 20 04:30:30 2016)
```

#When PC1 sends various non-attack ARP Request packets, and the sending rate is larger than or equal to the port-based speed limit threshold 100 and smaller than the port-based attack threshold 200, Device forms the related table entries and outputs the log information. Device identifies the port-based ARP overspeed.

```
Device#show aarf arp-guard ports
-------------------------------------------------------------------------------
----
Interface                   Hosts                Scan                 Action
                Policy
-------------------------------------------------------------------------------
----
te0/1                       0                    0                    overspeed
                monitor
```

#The output log is:

```
Dec 22 2016 06:36:32: %AARF-INTERFACE-3:<arp-guard>Interface te0/1 was overspeed.(THU DEC 22 06:36:29 2016)
```

#When PC1 sends various non-attack ARP Request packets, and the sending rate is larger than or equal to the port-based attack threshold 200, Device filters all ARP packets of the port, forms the related table entries and outputs the log information. Device identifies the port-based ARP attack.

```
Device#show aarf arp-guard ports
-------------------------------------------------------------------------------
----
Interface                   Hosts                Scan                 Action
                Policy
-------------------------------------------------------------------------------
----
te0/1                       0                    0                    attack
                filter
```

#The output log is:

```
Dec 22 2016 06:46:58: %AARF-INTERFACE-3:<arp-guard>Interface te0/1 was filter.(THU DEC
22 06:46:57 2016)
```

#When PC1 sends the ARP Request packet with the fixed MAC and increasing Sender IP, and the number of the ARP Request packets sent within 10s exceeds 15, form the related table entries, and output the log information. Device identifies the ARP MAC scanning.

```
Device#show aarf arp-guard scan
-------------------------------------------------------------------------------
----
Interface              Vlan                    IP                      MAC
                                Time-stamp
-------------------------------------------------------------------------------
----
te0/1                  2                       N/A                     0012.1011.0001    THU
DEC 22 03:16:30 2016
Total: 1 record(s).
```

#The output log is:

```
Dec 22 2016 03:16:19: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan
detected on interface te0/1.(THU DEC 22 03:16:16 2016)
Dec 22 2016 03:16:19: %AARF-SCAN-4:<arp-guard>Host<IP=N/A,MAC=0012.1011.0001,interface=
te0/1,VLAN=2> scan was detected.(THU DEC 22 03:16:16 2016)
```

#When PC1 sends the ARP Request packet with the fixed MAC and Sender IP, and the increasing Target IP, and the number of the ARP Request packets sent within 10s exceeds 15, form the related table entries, and output the log information. Device identifies the ARP MAC-IP scanning.

```
Device#show aarf arp-guard scan
-------------------------------------------------------------------------------
----------
Interface              Vlan                    IP                      MAC
                                Time-stamp
-------------------------------------------------------------------------------
----------
te0/1                  2              192.168.1.254           0012.1011.0001    THU DEC 22
03:38:52 2016
Total: 1 record(s).
```

#The output log is:

Dec 22 2016 03:37:33: %AARF-INTERFACE-3:<arp-guard>There are overspeed, attack or scan detected on interface te0/1.(THU DEC 22 03:37:30 2016)

Dec 22 2016 03:37:33:%AARF-SCAN-4:<arp-guard>Host<IP=192.168.1.254,MAC=0012.1011.0001, interface=te0/1,VLAN=2> scan was detected.(THU DEC 22 03:37:30 2016)

9.19 PPPoE+

9.19.1 Overview

PPPoE + (point point protocol over Ethernet plus) is also called PPPoE intermediate agent. This function is similar to DHCP option82. It expands the PPPoE protocol message. The access device intercepts the protocol packet in the PPPoE discovery stage, inserts the physical information of the client in the uplink direction, and peels off the physical information of the client in the downlink direction, so as to realize the identification of the client.

9.19.2 PPPoE + Principles

1. The access device with PPPoE + function enabled obtains the PADI packet sent by the PPPoE client and sends it to the PPPoE server after adding Vendor-Specific Tag to the load information field of the packet;
2. After receiving the PADI packet carrying Vendor-Specific Tag, the PPPoE server will return the PADO packet to the client;
3. PPPoE client sends PADR packet after receiving PADO packet;
4. The access device obtains the PADR packet, adds the Vendor-Specific Tag in the load information field of the packet and sends it to the PPPoE server;
5. When the PPPoE server receives the PADR packet with Vendor-Specific Tag, it will randomly generate a session-id, add it to the packet field of PADS and send it to the PPPoE client, so as to realize point-to-point PPP negotiation and PPPoE packet interaction with the client.

9.19.3 Brief Introduction to Vendor-Specific Tag of PPPoE Packet

This tag is used to transmit information customized by the manufacturer. In order

to enable the PPPoE server to obtain the physical information of the PPPoE client, the Vendor-Specific Tag can be added to the PPPoE request packet.

While interacting with PPPoE packet, the device can add some user related device information to PPPoE request packet in the form of Vendor-Specific Tag. The Vendor-Specific Tag records the physical information of the client, circuit-id is the circuit ID, and remote-id is the remote ID

When the PPPoE + function is enabled, after receiving the PPPoE request packet, the device can provide the following processing according to the processing policy and filling method of the Vendor-Specific Tag of the PPPoE packet configured by the user:

Table 1287 Processing policy of PPPoE request packet

PPPoE request packet	Processing policy	Filling Mode	Packet processing principle
Not carry Vendor-Specific Tag	add	Default filling mode	Fill in and forward according to the default format
	add	Extended filling mode	Fill in and forward by the customized format
Carry Vendor-Specific Tag	Keep	Not fill in	Do not process or forward the PPPoE packet
	Filter	Drop the packet	Drop the PPPoE packet
	Replace	Default filling format	Replace the original Vendor-Specific Tag content and forward by the default format
		Extended filling mode	Replace the original Vendor-Specific Tag and forward by the customized format

9.19.4 PPPoE + Basic Function Configuration

Table 1288 PPPoE+ function configuration list

Configuration Tasks	
Enable/disable the PPPoE+ function	Enable/disable the PPPoE+ function of the port
Configure the processing policy of the PPPoE+	Configure the processing policy of the

Configuration Tasks	
function for the PPPoE packet with Vendor-Specific Tag	PPPoE+ function for the PPPoE packet with Vendor-Specific Tag
Configure the circuit-id content in Vendor-Specific Tag	Configure the circuit-id content in Vendor-Specific Tag
Configure the remote-id content in Vendor-Specific Tag	Configure the remote-id content in Vendor-Specific Tag
Configure the filling policy of the PPPoE+ function for the PPPoE packet with Vendor-Specific Tag	Configure the filling policy of the PPPoE+ function for the PPPoE packet with Vendor-Specific Tag
Configure the vendor-id value in Vendor-Specific Tag	Configure the vendor-id value in Vendor-Specific Tag

9.19.4.1 Eable/Disable PPPoE+ Function

Configuration Conditions

None

Enable/Disable PPPoE+ Function

Table 1289 Enable/disable the PPPoE+ function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	Enable/disable the PPPoE + function in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	Enable/disable the PPPoE+ function in the aggregation group mode
Enable/disable the PPPoE+ function	pppoe relay enable/no pppoe relay enable	By default, disable the PPPoE+ function.

9.19.4.2 Configure the Processing Policy of PPPoE + Function for the PPPoE Packet with Vendor-Specific Tag

Configuration Conditions

None

Configure the Processing Policy of PPPoE + Function for the PPPoE Packet with Vendor-Specific Tag

Table 1290 Configure the processing policy of PPPoE + function for the PPPoE packet with Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	The configuration takes effect in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	The configuration takes effect in the aggregation group mode
Configure the processing policy for the PPPoE packet with Vendor-Specific Tag	pppoe relay information policy {keep|drop|replace}	By default, it is replace, replacing and forwarding the packet information field with Vendor-Specific Tag

Note

- The **pppoe relay information policy keep** command is to keep the PPPoE packet with Vendor-Specific Tag in the port/aggregation group mode and forward it.
- The **pppoe relay information policy drop** command is to drop the PPPoE packet with Vendor-Specific Tag in the port/aggregation group mode.
- The **pppoe relay information policy replace** command is to replace the Vendor-Specific Tag content of the PPPoE packet with vendor-id tag in the

port/aggregation group mode and forward it.

9.19.4.3 Configure circuit-id Content in Vendor-Specific Tag

Configuration Conditions

None

Configure circuit-id Content in Vendor-Specific Tag

Table 1291 Configure circuit-id Content in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	The configuration takes effect in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	The configuration takes effect in the aggregation group mode
Configure circuit-id Content	pppoe relay information format circuit-id{*LINE*|default}	By default, fill in vlan-interfance in the packet.

Note

- The **pppoe relay information format circuit-id LINE** command is used by the user to customize the circuit-id content.
- The **pppoe relay information format circuit-id default** command is used to fill in circuit-id as vlan-interface.

9.19.4.4 Configure remote-id Content in Vendor-Specific Tag

Configuration Conditions

None

Configure remote-id Content in Vendor-Specific Tag

Table 1292 Configure remote-id Content in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	The configuration takes effect in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	The configuration takes effect in the aggregation group mode
Configure remote-id Content	pppoe relay infotmation format remote-id{*LINE*|default }	By default, fill in the mac address of the device port in the packet.

Note

- The **pppoe relay information format remote-id LINE** command is used by the user to customize the remote-id content.
- The **pppoe relay information format remote-id default** command is used to fill in remote-id as switch-mac.

9.19.4.5 Configure the Filling Policy of PPPoE + Function for the PPPoE Packet with Vendor-Specific Tag

Configuration Conditions

None

Configure the Filling Policy of PPPoE + Function for the PPPoE Packet with Vendor-Specific Tag

Table 1293 Configure the filling policy of PPPoE + function for the PPPoE packet with Vendor-Specific Tag

Step	Command	Description

Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	The configuration takes effect in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	The configuration takes effect in the aggregation group mode
Configure the filling policy for the PPPoE packet with Vendor-Specific Tag	pppoe relay information encapsulation {circuit-id|remote-id|both}	By default, fill in circuit-id and remote-id.

9.19.4.6 Configure Filling vendor-id Value in Vendor-Specific Tag

Configuration Conditions

None

Configure Filling vendor-id Value in Vendor-Specific Tag

Table 1294 Configure filling vendor-id value in Vendor-Specific Tag

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface mode	interface *interface name*	The configuration takes effect in the port mode
Enter the port aggregation group	interface link-aggregation *link-aggregation-id*	The configuration takes effect in the aggregation group mode
Configure the vendor-id value	pppoe relay information vendor-id *vendor-id*	The value range is 0-4294967295. By default, vendor-id is 2011.

10 Reliability

10.1HA

10.1.1 Overview

HA (High Availability) is one high availability management platform on the device, providing the regular detection for some system faults, ensuring that the services are not interrupted.

10.1.2 HA Function Configuration

10.1.2.1 HA monitoring and maintaining

Table 1295 HA monitoring and maintaining

Command	Description
show ham job	Display the HA task processing node table of the local device

10.2 ULFD

10.2.1 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 spanning tree detection failure results in the topology calculation error.

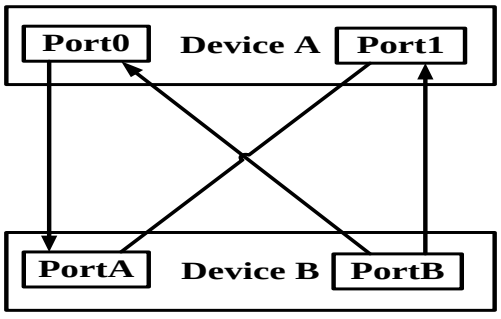


Figure 281 Fiber crossover connection

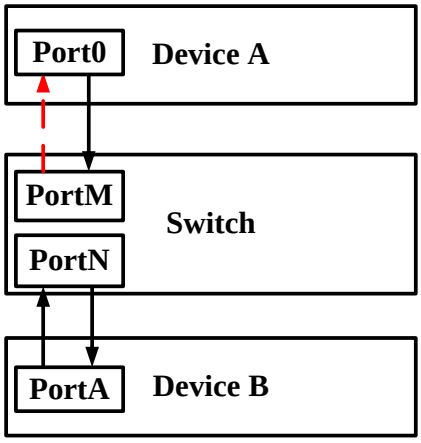


Figure 282 One fiber is not connection or disconnected

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.

10.2.2 ULFD Function Configuration

Table 1296 ULFD function configuration list

Configuration Task	
Configure the ULFD basic functions	Enable global ULFD function
	Enable the ULFD function of the Ethernet interface
Configure the ULFD parameters	Configure the period of sending the ULFD detection packets
	Re-set the Ethernet interface disabled by ULFD

10.2.2.1 Configure ULFD Basic Functions

Configuration Condition

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 1297 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 ULFD Function of Ethernet Interface

ULFD detection needs to enable the global ULFD detection function and the ULFD detection function of the Ethernet interface. If the ULFD function is not enabled globally, but just enabled on the Ethernet interface, the ULFD function cannot take effect.

If the global enabled ULFD detection mode and Ethernet interface enabled ULFD detection mode are inconsistent, the Ethernet interface ULFD detection mode takes effect first.

Table 1298 Enable the ULFD function of the Ethernet interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	-
Enable the ULFD function of the Ethernet interface	ulfd port [aggressive]	Mandatory By default, do not enable the ULFD function of the Ethernet

Step	Command	Description
		interface.

Note

- To switch over the ULFD work mode on the Ethernet interface, first cancel the previous work mode and then configure the new mode.
- When enabling the ULFD function on the Ethernet interface, ensure that the neighbor Ethernet interface is also configured with the ULFD function and works in the same detection mode.

10.2.2.2 Configure ULFD Parameters

Configuration Condition

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 1299 Configure the sending period of the ULFD detection packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
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 Ethernet Interface Disabled by ULFD

If ULFD detects the uni-direction and disables the Ethernet interface, to re-enable the ULFD detection function of the Ethernet interface, the user needs to perform the reset operation manually. The operation sets the Ethernet interface to UP and re-enables the ULFD detection.

Table 1300 Reset the Ethernet interface disabled by ULFD

Step	Command	Description
Reset the Ethernet interface disabled by ULFD	ulfd reset [interface *interface-name*]	Optional By default, do not execute the reset operation automatically after the Ethernet interface is disabled.

10.2.2.3 ULFD Monitoring and Maintaining

Table 1301 ULFD monitoring and maintaining

Command	Description
show ulfd [all | interface *interface-name* [detail]]	Display the ULFD global configuration information and all/specified Ethernet interface ULFD configuration information

10.2.3 ULFD Typical Configuration Example

10.2.3.1 Configure ULFD Basic Function

Network Requirements

- Device1 and Device2 are connected via the fiber.
- Configure the ULFD aggressive mode to disable the port when detecting the uni-directional link.

Network Topology

Figure 283 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 aggressive mode on port gigabitethernet0/1.

```
Device1#configure terminal
Device1(config)#ulfd aggressive
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ulfd port aggressive
Device1(config-if-gigabitethernet0/1)#exit
```

#Enable the ULFD function on Device2 and configure the ULFD work mode on port gigabitethernet0/1 as the aggressive mode.

```
Device2#configure terminal
Device2(config)#ulfd aggressive
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#ulfd port aggressive
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    : Aggressive
ULFD running mode   : Aggressive
Link status         : Link Up
Link direction      : Bidirectional
ULFD fsm status     : Advertisement

Neighbors number    : 1
----------
  Device ID         : 01017a787878
  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 (refer to Figure 2-1 and Figure 2-2), 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[01017a787878], device name[Device2], interface name[gigabitethernet0/1]!
%LINK-INTERFACE_DOWN-3: interface gigabitethernet0/1, changed state to down
%ULFD-UNDIR_LINK_ERR_V3-4: 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 common work mode is normal mode, refer to the configuration method. The normal mode only supports detecting the single-pass caused by the cross-connection of the fiber.

10.3 EIPS

10.3.1 Overview

In the Ethernet L2 network, STP is adopted for network reliability. STP is a standard ring protection protocol developed by the IEEE and extensively applied, but it is restricted by the actual network capacity and the convergence time is affected by the network topology. The STP convergence time is in the unit of second and a larger network diameter results in longer convergence time.

To reduce the convergence time and eliminate the impact of the network capacity, the EIPS (Ethernet Intelligent Protection Switching) emerges. The EIPS is a link layer protocol applied to the Ethernet ring and it can prevent the broadcast storm caused by the data link. When a link on the Ethernet ring is disconnected, a backup link can be used immediately to recover the communications among different nodes on the ring

network. Compared with the STP, the EIPS is characterized with faster topology convergence speed (less than 50s) and convergence time irrelevant with the number of the nodes on the ring network.

The EIPS supports the sub ring and hierarchical modes. In the sub ring mode, two intersecting rings are divided into a main ring and a sub ring. A common link exists between the main ring and sub ring. In the hierarchical mode, a main ring is selected from the intersecting rings. The low-level link is formed by the ring connected to the main ring excluding the common link with the main ring. Generally, the sub ring mode divides the intersecting rings to the main ring and sub ring, and the hierarchical mode divides the intersecting rings to the main ring and low-level link. In both modes, there is only one main ring and multiple sub rings or multiple low-level links.

10.3.1.1 Basic Concepts

To better understand the basic concepts introduced in this section, refer to the legends of the typical topologies of the sub ring mode and hierarchical mode.

1. EIPS domain

An EIPS domain is constructed by interconnected devices with the same domain ID and same control VLAN. It can contain multiple EIPS rings. One is the main ring and the others are the sub rings. An EIPS domain consists of EIPS ring, EIPS control VLAN, master node, transmission node, edge control node, and edge assistant node.

2. EIPS ring

An EIPS ring is identified by an integer ID, physically corresponding to an Ethernet topology in a ring. The EIPS ring includes a main ring and multiple sub rings. A sub ring is intersected with the main ring via the edge node and is intersected with the other sub rings via the main ring. The level of a main ring is 0 and the level of a sub ring is greater than 0.

3. EIPS node

Switches on the EIPS ring are called nodes. Each node has a unique domain ID

and ring ID, and is connected to the ring by two ports, one primary port and one secondary port specified by the user.

Master node: initiates the polling of the Ethernet ring status and implements the measures when the network topology status changes. Only one master node is available on a ring.

Transmission node: specifies the nodes excluding the master node on the EIPS main ring. It monitors the status of the link directly connected to the node and reports the status changes to the master node through the EIPS protocol packets. And then, the master node decides how to handle this situation.

The two nodes intersected by the sub ring and the main ring are called edge nodes (also called transmission node on the main ring). Edge nodes include the edge control node and edge assistant node, which should be used in pair to detect the integrity and fault status of the sub ring.

4. EIPS control VLAN

A control VLAN is used to transfer the EIPS protocol packets. All ports on the EIPS ring should be configured with control VLANs. The control VLAN interfaces cannot be configured with IP addresses. In the sub ring mode, the ports on the main ring should be added to both the control VLAN of the main ring and the control VLAN of the sub rings, but the ports on the sub ring can only be added to the control VLAN of the sub rings. In the hierarchical mode, the control VLANs can be the same on the main ring and on the low-level links.

5. EIPS port

The EIPS port is an abstract conception, corresponding to a link forming the EIPS ring. This link can be a single physical link or an aggregation port formed by multiple physical links. Each EIPS node has two ports connected to the EIPS ring. Due to the EIPS ring intersection, an EIPS port may belong to multiple EIPS nodes.

Primary EIPS port and secondary EIPS port: The ports on the master node and

transmission node are divided into the primary port and secondary port. The main port on the master node sends the Hello packet and the secondary port receives this packet. This method is used to ensure the ring integrity. If the ring is complete, the data VLAN of the secondary port of the master node is blocked. For a transmission node, a primary port and a secondary port do not have special meanings.

6. Topology level

Topology level refers to the hierarchical division of the rings in the EIPS domain. The EIPS domain comprises a ring or multiple intersecting rings. When the EIPS domain consists of only one single ring, the ring is the major-level ring and is numbered 0; when the EIPS domain comprises multiple intersecting rings, a ring is selected as the major-level ring and is numbered 0. The low-level segment link refers to the ring connected to the major-level ring excluding the common link intersecting with the major-level ring.

The low-level link refers to the link set excluding the common link connected to the upper layer.

The major-level ring is numbered 0 (the highest level). The lower the level is, the larger the level number is.

7. Topology segment

In a hierarchical EIPS, the segment number is used to identify different low-leve links of the same layer. Multiple low-level links may exist on the same level of the EIPS domain and are defined by different segment numbers. The segment number of the major-level ring is 0.

After the EIPS domain is divided by levels and segments, the corresponding ring or low-level link of each level and segment in the whole domain is identified by unique level number and segment number, which is called level segment. The low-level links defining the level number and segment number are called low-level segment.

10.3.1.2 Operating Mechanism

1. Polling mechanism

The polling mechanism is a mechanism that the master node of the EIPS ring actively detects the integrity of the ring.

The master node sends the Hello packet from the primary port periodically and the packets are transmitted over all transmission nodes. If the ring is healthy, the secondary port on the master node will receive the Hello packet before timing out and the master node will keep the secondary port in the blocked state. If the ring is broken, the secondary port on the master node cannot receive the Hello packet before timing out and the master node will unblock the data VLANs at the secondary port and send the COMM-FLUSH-FDB packet to all transmission nodes to update their own forwarding table entries.

2. Link-down alarm mechanism

When any port on the transmission node or the edge node is Down on the EIPS ring, it will send the Link-Down packet to the master node at once. When the master node receives the Link-Down packet, it unblocks the data VLANs at its secondary port and sends the COMM-FLUSH-FDB packet to all transmission nodes and edge nodes to update their own forwarding table entries. After the nodes update their forwarding table entries, the data flow is switched to a normal link.

3. Ring recovery mechanism

When any port on the transmission node or the edge node is Up again on the EIPS ring, the master node may discover the ring recovery after a period of time. The network may form a temporary ring and generate broadcast storm for data VLANs.

To prevent generating temporary ring, when the standby node finds its port connecting to the ring is Up again, the standby node temporarily blocks the port (only the packets of control VLANs are permitted to pass). When it is sure that no loop will be caused, the port is unblocked.

4. Load balancing mechanism

Multiple EIPS domains are configured on the same Ethernet ring and send the traffic of different data VLANs. That is, different VLAN traffics are forwarded along different paths, resulting in load balancing.

5. Standby node mechanism

The transmission node directly connected to the secondary port on the master node is considered as a standby node. When the master node operates normally, the standby node works as a transmission node; when the master node breaks down, the standby node works as a master node.

10.3.1.3 Typical Topology for Subring Mode

- Typical topology for the single ring

EIPS Domain1 includes one EIPS Ring1, Master, Transit1, Transit2, and Transit3, as shown in Figure 289.

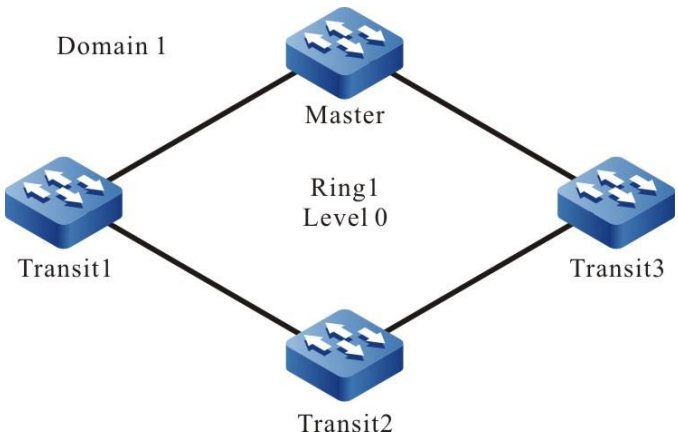


Figure 284 Topology for the single ring

This topology is characterized with fast response and short convergence time for topology changes.

- Typical topology for the intersecting ring

EIPS Domain1 includes two rings, Ring1 as the main ring and Ring2 as the sub ring. Ring1 consists of Master, Transit1, and Transit2; Ring2 consists of Edge control (Transit3), Edge assistant (Transit4), Sub Transit1, and Sub Transit2. Both Edge control

and Edge assistant are transmission nodes of Ring1, as shown in Figure 290.

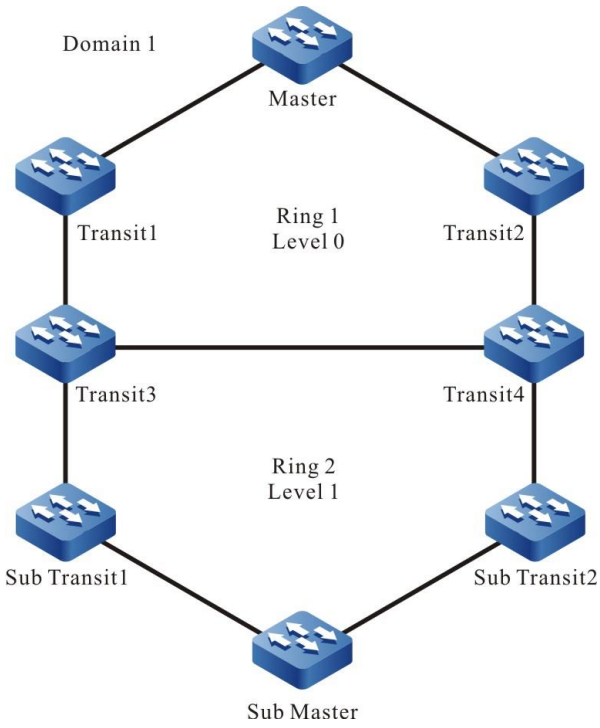


Figure 285 Topology for the intersecting ring

This topology is mainly applied to the scenario that a sub ring is dual homing to the uplink through two edge nodes, providing uplink backup.

10.3.1.4 Typical Topology for Hierarchical Mode

- Typical topology for the single ring

EIPS Domain1 includes Ring1, Master, Transit1, Transit2, and Transit3. The primary port (Primary) and secondary port (Slave) are configured on the master node. EIPS Domain1 has only Ring1. This single ring is defined as the major-level ring with level numbered 0 and segment numbered 0. When the major-level ring is not faulty, data VLANs on the port Slave are blocked. , as shown in Figure 3-3.

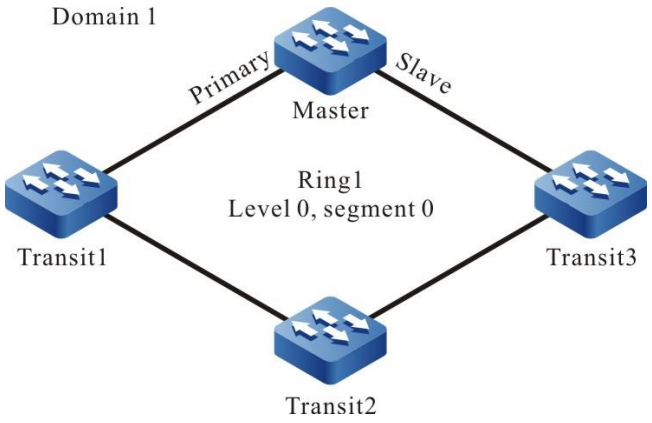


Figure 286 Topology for the single ring in the hierarchical mode

- Typical topology for the intersecting ring

Domain1 is divided into a hierarchical structure with a major-level ring and a low-level segment. Ring1 is defined with level numbered 0 and segment numbered 0. The ring intersected with Ring1 excludes the common parts caused by Transit2 and Transit3 intersection and forms a low-level segment with level numbered 1 and segment numbered 1.

The major-level ring (Level 0 and segment 0) includes Master, Transit1, Transit2, Transit3, and Transit4. The major-level ring is a single ring.The low-level segment (Level 1 and segment 1) includes Edge control (Transit2) and Edge assistant (Transit3), Transit5, and Transit6.

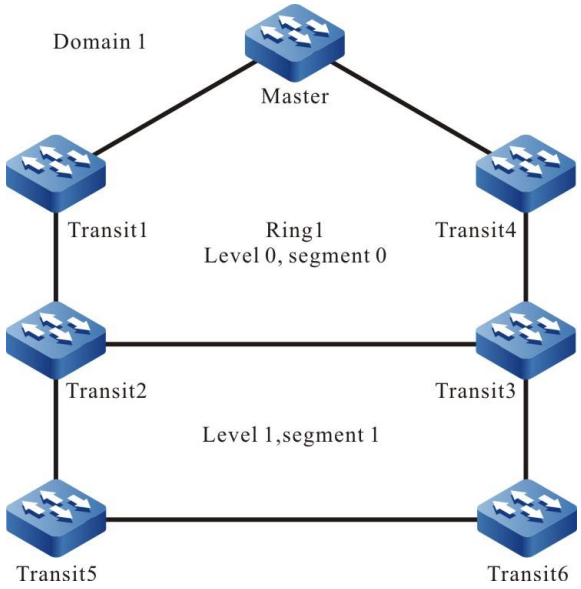


Figure 287 Topology for the intersecting ring in the hierarchical mode

10.3.2 EIPS Function Configuration

Table 1302 Configuration list of EIPS functions

Configuration Task	
Configure EIPS ring	Configure EIPS master node.
	Configure EIPS transmission node.
	Configure EIPS edge control node.
	Configure EIPS edge assistant node.
	Configure EIPS domain.
	Configure EIPS control VLAN.
	Configure EIPS level number.
	Configure EIPS segment number.
	Configure EIPS data instance.
Configure EIPS reliability	Configure EIPS standby node.
	Configure EIPS uni-directional detection.
Configure EIPS timer	Configure EIPS timer.

Note

- The EIPS supports both the sub ring mode and hierarchical mode.
- The hierarchical mode is recommended.
- The configuration in the hierarchical mode differs slightly from the configuration in the sub ring mode. The parameter **segment** and the EIPS segment number are compulsory for creating EIPS nodes in the hierarchical mode.

10.3.2.1 Configure EIPS Ring

Before configuring the EIPS ring, configure the ports on the nodes that will be connected to the EIPS ring and the nodes on the ring.

Configuration Conditions

Before configuring the EIPS ring, first complete the following tasks:

- Configure the type of ports that will be connected to nodes as nni.
- Disable the STP on ports that will be connected to nodes.
- Configure the mode of ports that will be connected to nodes as trunk.
- Add the ports that will be connected to nodes to the control VLAN that the node belongs to.

Configure EIPS Master Node

Perform the following configurations on the device that will be configured as the master node.

Table 1303 Configure the EIPS master node

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the EIPS master node	eips ring *ring-id* master [segment]	Mandatory By default, the EIPS master node is not configured. It is recommended that the segment parameter be used to specify the EIPS ring in the hierarchical mode. Otherwise, the EIPS ring is in the sub ring mode.
Configure the primary port on the master node	primary interface *interface-name*	Mandatory By default, the primary port on the master node is not configured.
Configure the secondary port of the master node	secondary interface *interface-name*	Mandatory By default, the secondary port on the master node is not configured.
Configure the data instance for the master node	instance *instance-id*	Mandatory By default, the data instance for

Step	Command	Description
		the master node is not configured. The data VLANs that are allowed to pass on the EIPS port must be contained in the EIPS data instance. The same data instance must be configured on all the nodes in the same EIPS domain.

Note

- In the sub ring mode, all ports on the main ring must be added to the control VLAN of the sub ring.

Configure EIPS Transmission Node

Perform the following configurations on the device that will be configured as the transmission node.

Table 1304 Configure the EIPS transmission node

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the EIPS transmission node	eips ring *ring-id* transit [segment]	Mandatory By default, the EIPS transmission node is not configured. It is recommended that the segment parameter be used to specify the EIPS ring in the hierarchical mode. Otherwise, the EIPS ring is in the sub ring mode.
Configure the primary port	primary interface *interface-*	Mandatory

Step	Command	Description
on the transmission node	*name*	By default, the primary port on the transmission node is not configured.
Configure the secondary port on the transmission node	secondary interface *interface-name*	Mandatory By default, the secondary port on the transmission node is not configured.
Configure the data instance for the transmission node	instance *instance-id*	Mandatory By default, the data instance for the transmission node is not configured. The data VLANs that are allowed to pass on the EIPS port must be contained in the EIPS data instance. The same data instance must be configured on all the nodes in the same EIPS domain.

Configure EIPS Edge Control Node

Perform the following configurations on the device that will be configured as the edge control node.

Table 1305 Configure the EIPS edge control node

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the edge control node	eips ring *ring-id* edge [segment]	Mandatory By default, the edge control node is not configured. It is recommended that the segment parameter be used to specify the EIPS ring in the hierarchical mode. Otherwise, the EIPS ring is in the sub ring

Step	Command	Description
		mode.
Associate the edge control node to the transmission node	transit ring *ring-id*	Mandatory By default, the edge control node is not associated to the transmission node. Only when the edge control node is associated to the transmission node, the low-level segment or sub ring can coordinate with the main ring.
Configure the edge port on the edge control node	edge interface *interface-name*	Mandatory By default, the edge port for the edge control node is not specified. The edge port connects a low-level segment or sub ring to the main ring.
Control the data instance for the edge control node	instance *instance-id*	Mandatory By default, the data instance for the edge control node is not configured. The data VLANs that are allowed to pass on the EIPS port must be contained in the EIPS data instance. The same data instance must be configured on all the nodes in the same EIPS domain.

Configure EIPS Edge Assistant Node

Perform the following configurations on the device that will be configured as the edge assistant node.

Table 1306 Configure the EIPS edge assistant node

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure edge assistant node	eips ring *ring-id* assistant [segment]	Mandatory By default, the edge assistant node is not configured, It is recommended that the segment parameter be used to specify the EIPS ring in the hierarchical mode. Otherwise, the EIPS ring is in the sub ring mode.
Associate the edge assistant node to the transmission node	transit ring *ring-id*	Mandatory By default, the edge assistant node is not associated to the transmission node. Only when the edge assistant node is associated to the transmission node, the low-level segment or sub ring can coordinate with the main ring.
Configure the edge port on the edge assistant node	edge interface *interface-name*	Mandatory By default, the edge port on the edge assistant node is not configured. The edge port connects a low-level segment or sub ring to the main ring.
Configure the data instance for the edge assistant node	instance *instance-id*	Mandatory By default, the data instance for the edge assistant node is not configured. The data VLANs that are allowed to pass on the EIPS

Step	Command	Description
		port must be contained in the EIPS data instance. The same data instance must be configured on all the nodes in the same EIPS domain.

Configure EIPS Domain

The EIPS domain specifies the domain that the EIPS ring or the level segment belongs to. All nodes in the same EIPS domain must be configured with the same domain ID.

Table 1307 Configure EIPS domain

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the EIPS domain	domain id *domain-id*	Mandatory By default, the EIPS domain is not configured.

Configure EIPS Control VLAN

Configure the control VLAN for an EIPS ring or the level segment before starting the EIPS protocol. All nodes on the same EIPS ring must be configured with the same control VLAN. Therefore, when configuring the control VLAN, choose the VLAN that has been created but not used by other L2 protocols. Otherwise, the configuration fails.

The EIPS control VLAN transfers EIPS protocol packets instead of data packets.

Table 1308 Configure EIPS control VLAN

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the EIPS control VLAN	control vlan *vlan-id*	Mandatory By default, the EIPS control VLAN is not configured.

Configure EIPS Level Number

The EIPS level number is an important symbol to distinguish the main ring from the sub ring or low-level segment. The level number of all the main rings is 0 and the level number of level-1 sub ring or the level-1 level segment is 1. The rest can be done in the same manner. All the nodes on the sub rings must be configured and the sub ring number of the same level or the level number of the same level segment must be the same.

Table 1309 Configure EIPS level number

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure sub ring or level segment number	level *level-id*	Mandatory By default, the level number for the sub ring or the level segment is not configured.

Configure EIPS Segment Number

The EIPS segment number is an important symbol in the hierarchical mode. The segment number of the main ring is 0 and the segment number on the low-level segment is defined by the user. The segment number must be configured for the level segment with level number greater than 0. Meanwhile, the segment number for the nodes on the

same level segment must be the same.

Table 1310 Configure the EIPS segment number

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the EIPS segment number	segment *segment-id*	Mandatory By default, the segment number for the level segment is not configured. This command is dedicated to the EIPS hierarchical mode and is not available for the sub ring mode. The segment number is configured on the edge control node, transmission assistant node, and transmission node for the low-level segment.

Configure EIPS Data Instance

The data instance must be configured before configuring the EIPS ring or the level segment. The data VLANs that are allowed to pass on the EIPS port must be contained in the EIPS data instance. The same data instance must be configured on all the nodes in the same EIPS domain.

The data instance is configured by using the MSTP (Multiple Spanning Tree Protocol Instance). Therefore, before configuring the EIPS ring or the level segment, configure the MSTP instance and the mapping relationship between the MSTP and the VLAN contained in the MATP.

Table 1311 Configure the EIPS data instance

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the MSTP configuration mode	spanning-tree mst configuration	-
Configure the MSTP instance	instance *instance-id* vlan *vlan-range*	Mandatory By default, the MSTP creates the instance 0 which contains all VLANs. Configure the MSTP instance and map the MSTP with the corresponding data VLAN.
Activate the MST domain parameter configuration	active configuration pending	Mandatory By default, the modified MST domain parameter will not take effect at once, but will take effect after executing the command.
Enter the global configuration mode	exit	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the EIPS data instance	instance *instance-id*	Mandatory By default, the EIPS data instance is not configured.

Start EIPS Protocol

When the preceding configurations complete, run the following commands to start the EIPS protocol.

Table 1312 Start the protocol on the EIPS node

Step	Command	Description
Enter the global	configure terminal	-

Step	Command	Description
configuration mode		
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Start the EIPS protocol	eips start	Mandatory By default, the EIPS protocol on the nodes is not started.

10.3.2.2 Configure EIPS Reliability

Configuration Condition

No

Configure EIPS Standby Node

To improve the EIPS ring reliability, the standby node works by replacing the master node when the master node breaks down.

The standby node is configured on the transmission node that is directly connected to the master node.

Table 1313 Configure EIPS standby node

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the specified transmission node as standby node	backup master	Mandatory By default, the standby node is not configured.

Configure EIPS Uni-directional Detection

Enable the uni-directional detection function on the port or the port group.

Table 1314 Configure the EIPS uni-directional detection on the port

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure EIPS uni-directional detection on the port	eips udld interval [*value*]	Mandatory By default, the uni-directional detection function on the port is not enabled.

10.3.2.3 Configure EIPS Timer

Configuration Condition

Before configuring the EIPS timer, first complete the following task:

- Configure EIPS basic functions.

Configure EIPS Timer

For the master nodes and edge control nodes in the hierarchical mode, a timer is used to control the sending frequency and the timeout for receiving the Hello packet. For the transmission nodes, a block timer is used to control the duration for the transmission node transiting from the fault recovery status to the complete status.

Table 1315 Configure EIPS timer

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EIPS configuration mode	eips ring *ring-id* { master | transit | edge | assistant } [segment]	-
Configure the timer for EIPS node	timer { hello | receive | block } *timer-value*	Mandatory By default, the timeout of the hello timer is 1s; for the receiving timer, it is 5s; for the blocking timer, it is 10s.

Note

- The timer for sending the hello packet can be configured only on the master nodes or the edge control nodes and the blocking timer can be configure only on the transmission nodes.

Caution

- If the standby nodes are configured, the timeout duration for the Hello timer on the master nodes cannot be configured as 0.

10.3.2.4 EIPS Monitoring and Maintaining

Table 1316 EIPS monitoring and maintaining

Command	Description
clear eips { interface [*interface-name*] | interface link-aggregation [*link-aggregation-number*] | ring [*ring-id*] | udld }	Clear the EIPS-related statistics information
show eips { config [*ring-id*] | interface [*interface-name*] | interface link-aggregation [*link-aggregation-number*] | mac-control-table | ring [*ring-id*] | ticktimer [*ticktime-name*] | topology [ring *ring-id*] | topology-summary [ring *ring-id*] | udld [interface *interface-name*] }	Display the EIPS configuration information, status, and statistics information, including the EIPS port, aggregation port, address table, node, topology, timer information, and UDLD uni-directional audio related information

10.3.3 Typical Configuration Example of EIPS

10.3.3.1 Configure EIPS Single Ring in Hierarchical Mode

Network Requirements

- Four devices in the LAN are within the EIPS Ring 1. Configure the EIPS

hierarchy segment mode and block the secondary port gigabitethernet0/2 on Master to achieve the ring protection.

- When the link between the transmission node Transit1 and Transit2 is disconnected, unblock the STP blocked status for gigabitethernet0/2 on the Master node to achieve data switchover and ensure the communications in the LAN not affected.

Network Topology

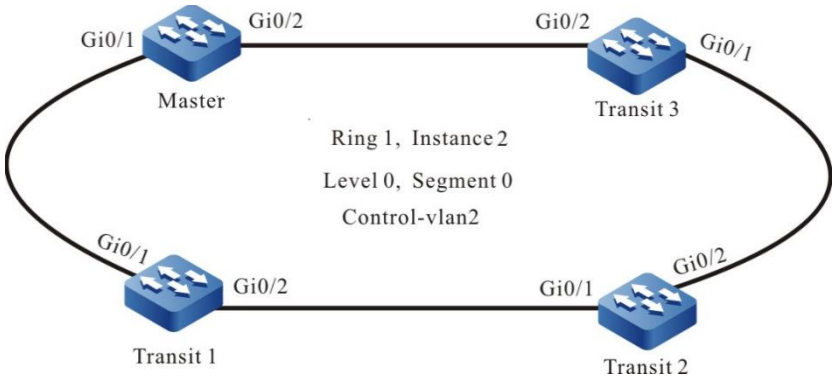


Figure 288 Networking of configuring the EIPS single ring in the hierarchical mode

Configuration Steps

Step 1: Configure the VLAN and port link type.

#Create VLAN2 and VLAN3 on Master and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2 and VLAN3 to pass. Configure the PVID as 1.

```
Master#configure terminal
Master(config)#vlan 2-3
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1
```

#Map VLAN3 on Master to the STP instance 2. Disable the STP and storm suppression on the ports gigabitethernet0/1 and gigabitethernet0/2.

```
Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
```

```
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit
```

#Create VLAN2 and VLAN3 on Transit1, and map VLAN3 to the STP instance 2. Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2 and VLAN3 to pass. Configure the PVID as 1. Disable the STP and storm suppression on ports gigabitethernet0/1 and gigabitethernet0/2. (Omitted)

#Create VLAN2 and VLAN3 on Transit2, and map VLAN3 to the STP instance 2. Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2 and VLAN3 to pass. Configure the PVID as 1. Disable the STP and storm suppression on ports gigabitethernet0/1 and gigabitethernet0/2. (Omitted)

#Create VLAN2 and VLAN3 on Transit3, and map VLAN3 to the STP instance 2. Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2 and VLAN3 to pass. Configure the PVID as 1. Disable the STP and storm suppression on ports gigabitethernet0/1 and gigabitethernet0/2. (Omitted)

Note

- VLAN2 is the control VLAN, which is only used to transfer the EIPS protocol packets. VLAN3 is the data VLAN, which is used to transfer services.
- To enable the EIPS function, the data VLAN of the EIPS must be mapped

to the corresponding STP instance and the STP function on the port must be disabled.

Step 2: Configure the EIPS hierarchical mode

#Create the main ring master node Ring1 in the hierarchical mode on Master. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Master(config)#eips ring 1 master segment
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#segment 0
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#Create the transmission node Ring1 in the hierarchical mode on Transit1. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Transit1(config)#eips ring 1 transit segment
Transit1(config-eips)#control vlan 2
Transit1(config-eips)#level 0
Transit1(config-eips)#segment 0
Transit1(config-eips)#instance 2
Transit1(config-eips)#primary interface gigabitethernet 0/1
Transit1(config-eips)#secondary interface gigabitethernet 0/2
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#Create the transmission node Ring1 in the hierarchical mode on Transit2. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Transit2(config)#eips ring 1 transit segment
Transit2(config-eips)#control vlan 2
Transit2(config-eips)#level 0
Transit2(config-eips)#segment 0
Transit2(config-eips)#instance 2
Transit2(config-eips)#primary interface gigabitethernet 0/1
Transit2(config-eips)#secondary interface gigabitethernet 0/2
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#Create the transmission node Ring3 in the hierarchical mode on Transit3. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Transit3(config)#eips ring 1 transit segment
Transit3(config-eips)#control vlan 2
Transit3(config-eips)#level 0
Transit3(config-eips)#segment 0
Transit3(config-eips)#instance 2
Transit3(config-eips)#primary interface gigabitethernet 0/1
Transit3(config-eips)#secondary interface gigabitethernet 0/2
Transit3(config-eips)#eips start
Transit3(config-eips)#exit
```

Step 3: Check the result

#Run the **show eips topology-summary** command on the four devices. We can view that the EIPS ring status is round and the topology information is consistent.

```
Master#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1    Transit3       0000.0000.008b  transit   gi0/2          UP     gi0/1          UP     NO
 2    Transit2       0101.7a22.2224  transit   gi0/2          UP     gi0/1          UP     YES
 3    Transit1       0000.0010.0017  transit   gi0/2          UP     gi0/1          UP     YES
 4    Master         0101.7a54.5d71  master    gi0/1          UP     gi0/2          UP     NO

Transit3#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
```

```
-------------------------------------------------------------------------------
--------------------------
1   Master        0101.7a54.5d71  master   gi0/2          UP     gi0/1          UP     NO
2   Transit1      0000.0010.0017  transit  gi0/1          UP     gi0/2          UP     YES
3   Transit2      0101.7a22.2224  transit  gi0/1          UP     gi0/2          UP     YES
4   Transit3      0000.0000.008b  transit   gi0/1         UP     gi0/2          UP     NO

Transit1#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
-------------------------------------------------------------------------------
--------------------------
1   Transit2      0101.7a22.2224  transit  gi0/1          UP     gi0/2          UP     YES
2   Transit3      0000.0000.008b  transit   gi0/1         UP     gi0/2          UP     NO
3   Master        0101.7a54.5d71  master   gi0/2          UP     gi0/1          UP     NO
4   Transit1      0000.0010.0017  transit  gi0/1          UP     gi0/2          UP     YES

Transit2#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
-------------------------------------------------------------------------------
--------------------------
1   Transit3      0000.0000.008b  transit   gi0/1         UP     gi0/2          UP     NO
2   Master        0101.7a54.5d71  master   gi0/2          UP     gi0/1          UP     NO
3   Transit1      0000.0010.0017  transit  gi0/1          UP     gi0/2          UP     YES
4   Transit2      0101.7a22.2224  transit  gi0/1          UP     gi0/2          UP     YES
```

#Run the **show eips topology** command on the four devices. We can view that the secondary port gigabitethernet0/2 on Master is blocked and other ports are unblocked.

```
Master#show eips topology
 ring ID     : 1
 topo status  : round
 topo index 1  :
      host name      : Transit3
      eips type      : transit
      eips status    : COMPLETE
      border         : NO
      base MAC       : 0000.0000.008b
      sys oid        : 1.3.6.1.4.1.59955.1.102.146
      interface1     : gi0/2
        MAC          : 0000.0000.008b
        role         : second
```

```
        block-status    : unblock
        link-status     : UP
      interface2      : gi0/1
        MAC           : 0000.0000.008b
        role          : primary
        block-status    : unblock
        link-status     : UP
topo index 2   :
    host name       : Transit2
    eips type       : transit
    eips status     : COMPLETE
    border          : YES
    base MAC        : 0101.7a22.2224
    sys oid         : 1.3.6.1.4.1.59955.1.102.146
    interface1      : gi0/2
      MAC           : 0101.7a22.2224
      role          : second
      block-status    : unblock
      link-status     : UP
    interface2      : gi0/1
      MAC           : 0101.7a22.2224
      role          : primary
      block-status    : unblock
      link-status     : UP
topo index 3   :
    host name       : Transit1
    eips type       : transit
    eips status     : COMPLETE
    border          : YES
    base MAC        : 0000.0010.0017
    sys oid         : 1.3.6.1.4.1.59955.1.102.140
    interface1      : gi0/2
      MAC           : 0000.0010.0017
      role          : second
      block-status    : unblock
      link-status     : UP
    interface2      : gi0/1
      MAC           : 0000.0010.0017
      role          : primary
      block-status    : unblock
      link-status     : UP
topo index 4   :
    host name       : Master
    eips type       : master
    eips status     : COMPLETE
```

```
    border        : NO
    base MAC      : 0101.7a54.5d71
    sys oid       : 1.3.6.1.4.1.59955.1.102.145
    interface1    : gi0/1
     MAC          : 0101.7a54.5d71
     role         : primary
     block-status : unblock
     link-status  : UP
    interface2    : gi0/2
     MAC          : 0101.7a54.5d71
     role         : second
     block-status : block
     link-status  : UP
```

#When the link between Transit1 and Transit2 is disconnected, run the **show eips topology** command again. We can view that the ring status changes to not round, EIPS status is FAULT, and the secondary port gigabitethernet0/2 on Master changes to unblock. Transit1 communicates with Transit2 via Master, which ensures uninterrupted communications between Transit1 and Transit2.

```
Master#show eips topology
 ring ID     : 1
 topo status : not round
 topo index 1  :
      host name     : Transit1
      eips type     : transit
      eips status   : FAULT
      border        : YES
      base MAC      : 0000.0010.0017
      sys oid       : 1.3.6.1.4.1.59955.1.102.140
      interface1    : gi0/2
       MAC          : 0000.0010.0017
       role         : second
       block-status : block
       link-status  : DOWN
      interface2    : gi0/1
       MAC          : 0000.0010.0017
       role         : primary
       block-status : unblock
       link-status  : UP
 topo index 2  :
      host name     : Master
      eips type     : master
      eips status   : FAULT
```

```
        border         : NO
        base MAC       : 0101.7a54.5d71
        sys oid        : 1.3.6.1.4.1.59955.1.102.145
        interface1     : gi0/1
          MAC          : 0101.7a54.5d71
          role         : primary
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/2
          MAC          : 0101.7a54.5d71
          role         : second
          block-status    : unblock
          link-status     : UP
    topo index 3   :
        host name      : Transit3
        eips type      : transit
        eips status    : FAULT
        border         : NO
        base MAC       : 0000.0000.008b
        sys oid        : 1.3.6.1.4.1.59955.1.102.146
        interface1     : gi0/2
          MAC          : 0000.0000.008b
          role         : second
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/1
          MAC          : 0000.0000.008b
          role         : primary
          block-status    : unblock
          link-status     : UP
    topo index 4   :
        host name      : Transit2
        eips type      : transit
        eips status    : FAULT
        border         : YES
        base MAC       : 0101.7a22.2224
        sys oid        : 1.3.6.1.4.1.59955.1.102.146
        interface1     : gi0/2
          MAC          : 0101.7a22.2224
          role         : second
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/1
          MAC          : 0101.7a22.2224
          role         : primary
```

```
block-status    : block
link-status     : DOWN
```

10.3.3.2 Configure EIPS Intersecting Rings in Hierarchical Mode

Network Requirements

- Six devices in the LAN form two-level intersecting rings. Configure the EIPS hierarchical mode to block the secondary port gigabitethernet0/2 on Master and the edge port gigabitethernet0/3 on Transit 1 to achieve the ring protection.
- When the link between Transit1 and Transit2 is disconnected, unblock the STP blocked status for gigabitethernet0/2 on Master of the main ring to achieve data switchover and ensure the communications in Ring1 not affected.
- When the link between sTransit1 and sTransit2 is disconnected, unblock the STP blocked status for gigabitethernet0/3 on Transit1 to achieve data switchover and ensure the communications in Ring2 not affected.

Network Topology

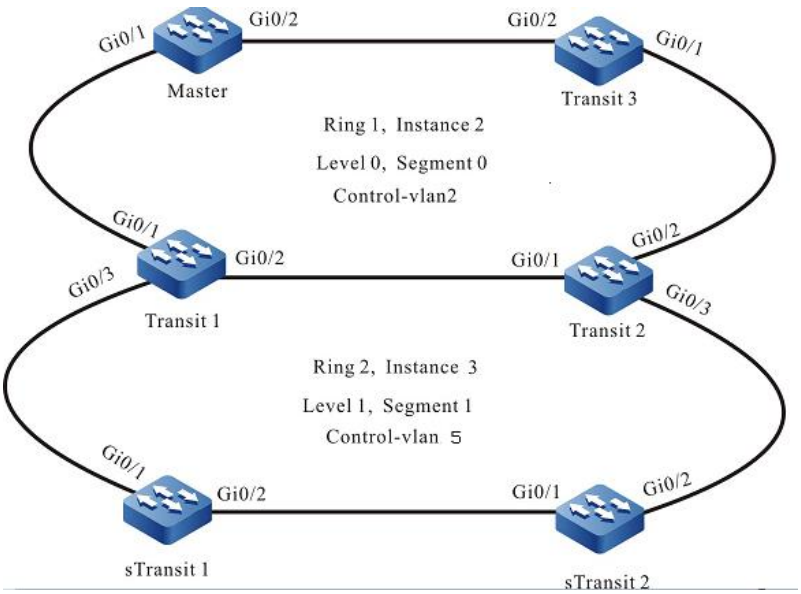


Figure 289 Networking of configuring the EIPS intersecting ring in the hierarchical mode

Configuration Steps

Step 1: Configure VLAN and port link type.

#Create VLAN2 and VLAN3 on Master. Configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2 and VLAN3 to pass. Configure the PVID as 1.

```
Master#configure terminal
Master(config)#vlan 2-3
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1
```

#Map VLAN3 on Master to the STP instance 2. Disable the STP and storm suppression on ports gigabitethernet0/1 and gigabitethernet0/2.

```
Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit
```

#Create VLAN2-5 on the master ring transmission node transit1, map vlan3 to spanning tree instance 2, and map vlan4 to spanning tree instance 3. Configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk to allow vlan2-3 services to pass through, and configure the link type of ports gigabitethernet0/2-gigabitethernet0/3 as trunk to allow vlan4-5 services to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/3. (omitted)

#Create vlan2-5 on the master ring transmission node transit2, map vlan3 to spanning tree instance 2, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan2-3 to pass, and configure PVID as 1. Configure the link type of ports gigabitethernet0/2-gigabitethernet0/3 as trunk, allow vlan4-5 services to pass, and configure PVID as 1. Disable spanning tree and storm suppression functions on ports gigabitethernet0/1-gigabitethernet0/3. (omitted)

#Create vlan2 and vlan3 on the master ring transmission node transit3, map vlan3 to spanning tree instance 2, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan2 and vlan3 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

#Create vlan4 and vlan5 on the primary sub ring transmission node stransit1, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan4 and vlan5 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

#Create vlan4 and vlan5 on the primary sub ring transmission node stransit2, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan4 and vlan5 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

Note

- VLAN5 is the control VLAN, which is only used to transfer the EIPS protocol packets. VLAN4 is the data VLAN, which is used to transfer services.

- To enable the EIPS function, the data VLAN of the EIPS must be mapped to the corresponding STP instance and the STP and storm suppression function on the port must be disabled.

Step 2: Configure Ring1.

#Create the master node Ring1 in the hierarchical mode on Master. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Master(config)#eips ring 1 master segment
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#segment 0
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#Create transmission node Ring1 in the hierarchical mode on Transit1. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS. (Omitted)

Create transmission node Ring1 in the hierarchical mode on Transit2. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS. (Omitted)

Create transmission node Ring1 in the hierarchical mode on Transit3. Configure the level number of the EIPS ring as 0, segment number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS. (Omitted)

Step 3: Configure Ring2.

#Create edge node Ring2 in the hierarchical mode on Transit1. Configure the level number of the EIPS ring as 1, segment number as 1, instance as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3, and Ring1 as its associated transmission node. Enable the EIPS.

```
Transit1(config)#eips ring 2 edge segment
Transit1(config-eips)#control vlan 5
Transit1(config-eips)#level 1
Transit1(config-eips)#segment 1
Transit1(config-eips)#instance 3
Transit1(config-eips)#transit ring 1
Transit1(config-eips)#edge interface gigabitethernet0/3
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#Create the edge node Ring2 in the hierarchical mode on Transit2. Configure the level number of the EIPS ring as 1, segment number as 1, instance as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3, and Ring1 as its associated transmission node. Enable the EIPS.

```
Transit2(config)#eips ring 2 assistant segment
Transit2(config-eips)#control vlan 5
Transit2(config-eips)#level 1
Transit2(config-eips)#segment 1
Transit2(config-eips)#instance 3
Transit2(config-eips)#transit ring 1
Transit2(config-eips)#edge interface gigabitethernet0/3
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#Create the transmission node Ring2 in the hierarchical mode on sTransit1. Configure the level number of the EIPS ring as 1, segment number as 1, instance as 3, control VLAN as VLAN5, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
sTransit1(config)#eips ring 2 transit segment
sTransit1(config-eips)#control vlan 5
sTransit1(config-eips)#level 1
```

```
sTransit1(config-eips)#segment 1
sTransit1(config-eips)#instance 3
sTransit1(config-eips)#primary interface gigabitethernet 0/1
sTransit1(config-eips)#secondary interface gigabitethernet 0/2
sTransit1(config-eips)#eips start
sTransit1(config-eips)#exit
```

Create the transmission node Ring2 in the hierarchical mode on sTransit2. Configure the level number of the EIPS ring as 1, segment number as 1, instance as 3, control VLAN as VLAN5, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
sTransit2(config)#eips ring 2 transit segment
sTransit2(config-eips)#control vlan 5
sTransit2(config-eips)#level 1
sTransit2(config-eips)#segment 1
sTransit2(config-eips)#instance 3
sTransit2(config-eips)#primary interface gigabitethernet 0/1
sTransit2(config-eips)#secondary interface gigabitethernet 0/2
sTransit2(config-eips)#eips start
sTransit2(config-eips)#exit
```

Step 4: Check the result.

Run the show eips topology-summary command on the edge node and assistant node. We can view that the EIPS status of the main ring and sub rings is round and the topology information is consistent.

```
Transit1#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1   Transit2       0101.7a22.2224  transit   gi0/1          UP     gi0/2          UP     YES
 2   Transit3       0000.0000.008b  transit   gi0/1          UP     gi0/2          UP     NO
 3   Master         0014.0000.1202  master    gi0/2          UP     gi0/1          UP     NO
 4   Transit1       0101.7a54.5d71  transit   gi0/1          UP     gi0/2          UP     YES

 ring ID     : 2
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
```

```
1   Transit2       0101.7a22.2224  assistant ----          ----   gi0/3        UP     NO
2   sTransit2      2012.1209.1728  transit   gi0/2         UP     gi0/1        UP     NO
3   sTransit1      0000.0010.0017  transit   gi0/2         UP     gi0/1        UP     NO
4   Transit1       0101.7a54.5d71  edge      gi0/3         UP     ----         ----   NO

Transit2#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1   Transit3       0000.0000.008b  transit   gi0/1         UP     gi0/2        UP     NO
 2   Master         0014.0000.1202  master    gi0/2         UP     gi0/1        UP     NO
 3   Transit1       0101.7a54.5d71  transit   gi0/1         UP     gi0/2        UP     YES
 4   Transit2       0101.7a22.2224  transit   gi0/1         UP     gi0/2        UP     YES

 ring ID     : 2
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1   Transit1       0101.7a54.5d71  edge      ----          ----   gi0/3        UP     NO
 2   sTransit1      0000.0010.0017  transit   gi0/1         UP     gi0/2        UP     NO
 3   sTransit2      2012.1209.1728  transit   gi0/1         UP     gi0/2        UP     NO
 4   Transit2       0101.7a22.2224  assistant gi0/3         UP     ----         ----   NO
```

#Run the **show eips topology** command on the edge port. We can view that the secondary port gigabitethernet0/2 on Master and edge port gigabitethernet0/3 on Transit1 are blocked and the other ports are unblocked. The EIPS status of the main ring and sub rings is COMPLETE.

```
Transit1#show eips topology
 ring ID     : 1
 topo status  : round
 topo index 1   :
       host name      : Transit2
       eips type      : transit
       eips status    : COMPLETE
       border         : YES
       base MAC       : 0101.7a22.2224
       sys oid        : 1.3.6.1.4.1.59955.1.0.0
       interface1     : gi0/1
        MAC           : 0101.7a22.2224
        role          : primary
```

```
        block-status    : unblock
        link-status     : UP
      interface2      : gi0/2
        MAC           : 0101.7a22.2224
        role          : second
        block-status    : unblock
        link-status     : UP
topo index 2   :
    host name       : Transit3
    eips type       : transit
    eips status     : COMPLETE
    border          : NO
    base MAC        : 0000.0000.008b
    sys oid         : 1.3.6.1.4.1.59955.1.102.146
    interface1      : gi0/1
      MAC           : 0000.0000.008b
      role          : primary
      block-status    : unblock
      link-status     : UP
    interface2      : gi0/2
      MAC           : 0000.0000.008b
      role          : second
      block-status    : unblock
      link-status     : UP
topo index 3   :
    host name       : Master
    eips type       : master
    eips status     : COMPLETE
    border          : NO
    base MAC        : 0014.0000.1202
    sys oid         : 1.3.6.1.4.1.59955.1.102.127
    interface1      : gi0/2
      MAC           : 0014.0000.1202
      role          : second
      block-status    : block
      link-status     : UP
    interface2      : gi0/1
      MAC           : 0014.0000.1202
      role          : primary
      block-status    : unblock
      link-status     : UP
topo index 4   :
    host name       : Transit1
    eips type       : transit
    eips status     : COMPLETE
```

```
        border         : YES
        base MAC       : 0101.7a54.5d71
        sys oid        : 1.3.6.1.4.1.59955.1.102.145
        interface1     : gi0/1
          MAC          : 0101.7a54.5d71
          role         : primary
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/2
          MAC          : 0101.7a54.5d71
          role         : second
          block-status    : unblock
          link-status     : UP

ring ID     : 2
topo status  : round
topo index 1   :
        host name      : Transit2
        eips type      : assistant
        eips status    : COMPLETE
        border         : NO
        base MAC       : 0101.7a22.2224
        sys oid        : 1.3.6.1.4.1.59955.1.0.0
        interface2     : gi0/3
          MAC          : 0101.7a22.2224
          role         : edge
          block-status    : unblock
          link-status     : UP
topo index 2   :
        host name      : sTransit2
        eips type      : transit
        eips status    : COMPLETE
        border         : NO
        base MAC       : 2012.1209.1728
        sys oid        : 1.3.6.1.4.1.59955.1.102.126
        interface1     : gi0/2
          MAC          : 2012.1209.1728
          role         : second
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/1
          MAC          : 2012.1209.1728
          role         : primary
          block-status    : unblock
          link-status     : UP
```

```
topo index 3   :
      host name      : sTransit1
      eips type      : transit
      eips status    : COMPLETE
      border         : NO
      base MAC       : 0000.0010.0017
      sys oid        : 1.3.6.1.4.1.59955.1.102.140
      interface1     : gi0/2
       MAC           : 0000.0010.0017
       role          : second
       block-status  : unblock
       link-status   : UP
      interface2     : gi0/1
       MAC           : 0000.0010.0017
       role          : primary
       block-status  : unblock
       link-status   : UP
topo index 4   :
      host name      : Transit1
      eips type      : edge
      eips status    : COMPLETE
      border         : NO
      base MAC       : 0101.7a54.5d71
      sys oid        : 1.3.6.1.4.1.59955.1.102.145
      interface1     : gi0/3
       MAC           : 0101.7a54.5d71
       role          : edge
       block-status  : block
       link-status   : UP
```

#When the link between Transit1 and Transit2 is disconnected, run the **show eips topology** command again. We can view that the status of Ring1 changes to not round, EIPS status changes to FAULT, gigabitethernet0/2 on Master changes to unblock. Transit1 communicates with Transit2 via Master, which ensures uninterrupted communications between Transit1 and Transit2. The status of Ring2 is still round, EIPS status is still COMPLETE, and gigabitethernet0/3 on Transit1 is still blocked.

```
Transit1#show eips topology ring 1
 ring ID     : 1
 topo status  : not round
 topo index 1   :
      host name      : Transit2
```

eips type : transit
eips status : FAULT
border : YES
base MAC : 0101.7a22.2224
sys oid : 1.3.6.1.4.1.59955.1.0.0
interface1 : gi0/1
MAC : 0101.7a22.2224
role : primary
block-status : block
link-status : DOWN
interface2 : gi0/2
MAC : 0101.7a22.2224
role : second
block-status : unblock
link-status : UP
topo index 2 :
host name : Transit3
eips type : transit
eips status : FAULT
border : NO
base MAC : 0000.0000.008b
sys oid : 1.3.6.1.4.1.59955.1.102.146
interface1 : gi0/1
MAC : 0000.0000.008b
role : primary
block-status : unblock
link-status : UP
interface2 : gi0/2
MAC : 0000.0000.008b
role : second
block-status : unblock
link-status : UP
topo index 3 :
host name : Master
eips type : master
eips status : FAULT
border : NO
base MAC : 0014.0000.1202
sys oid : 1.3.6.1.4.1.59955.1.102.127
interface1 : gi0/2
MAC : 0014.0000.1202
role : second
block-status : unblock
link-status : UP
interface2 : gi0/1

```
        MAC          : 0014.0000.1202
        role         : primary
        block-status   : unblock
        link-status    : UP
    topo index 4   :
      host name      : Transit1
      eips type      : transit
      eips status    : FAULT
      border         : YES
      base MAC       : 0101.7a54.5d71
      sys oid        : 1.3.6.1.4.1.59955.1.102.145
      interface1     : gi0/1
        MAC          : 0101.7a54.5d71
        role         : primary
        block-status   : unblock
        link-status    : UP
      interface2     : gi0/2
        MAC          : 0101.7a54.5d71
        role         : second
        block-status   : block
        link-status    : DOWN

Transit1#show eips topology ring 2
 ring ID     : 2
 topo status  : round
 topo index 1   :
      host name      : Transit2
      eips type      : assistant
      eips status    : COMPLETE
      border         : NO
      base MAC       : 0101.7a22.2224
      sys oid        : 1.3.6.1.4.1.59955.1.0.0
      interface2     : gi0/3
        MAC          : 0101.7a22.2224
        role         : edge
        block-status   : unblock
        link-status    : UP
 topo index 2   :
      host name      : sTransit2
      eips type      : transit
      eips status    : COMPLETE
      border         : NO
      base MAC       : 2012.1209.1728
      sys oid        : 1.3.6.1.4.1.59955.1.102.126
      interface1     : gi0/2
```

```
        MAC          : 2012.1209.1728
        role         : second
        block-status   : unblock
        link-status    : UP
      interface2     : gi0/1
        MAC          : 2012.1209.1728
        role         : primary
        block-status   : unblock
        link-status    : UP
topo index 3   :
    host name      : sTransit1
    eips type      : transit
    eips status    : COMPLETE
    border         : NO
    base MAC       : 0000.0010.0017
    sys oid        : 1.3.6.1.4.1.59955.1.102.140
    interface1     : gi0/2
      MAC          : 0000.0010.0017
      role         : second
      block-status   : unblock
      link-status    : UP
    interface2     : gi0/1
      MAC          : 0000.0010.0017
      role         : primary
      block-status   : unblock
      link-status    : UP
topo index 4   :
    host name      : Transit1
    eips type      : edge
    eips status    : COMPLETE
    border         : NO
    base MAC       : 0101.7a54.5d71
    sys oid        : 1.3.6.1.4.1.59955.1.102.145
    interface1     : gi0/3
      MAC          : 0101.7a54.5d71
      role         : edge
      block-status   : block
      link-status    : UP
```

#When only the link between sTransit1 and sTransit2 is disconnected, run the **show eips topology** command on the edge node and edge assistant node. We can view that the status of Ring2 changes to not round, EIPS status changes to FAULT, gigabitethernet0/3 on Transit1 changes to unblock. sTransit1 communicates with

sTransit2 via Transit1, which ensures uninterrupted communications between sTransit1 and sTransit2. The status of Ring1 is still round, EIPS status is still COMPLETE, and gigabitethernet0/2 on Master is still blocked.

```
Transit1#show eips topology ring 2
 ring ID     : 2
 topo status  : not round
 topo index 1   :
      host name      : sTransit1
      eips type      : transit
      eips status    : FAULT
      border         : NO
      base MAC       : 0000.0010.0017
      sys oid        : 1.3.6.1.4.1.59955.1.102.140
      interface1     : gi0/2
        MAC          : 0000.0010.0017
        role         : second
        block-status   : block
        link-status    : DOWN
      interface2     : gi0/1
        MAC          : 0000.0010.0017
        role         : primary
        block-status   : unblock
        link-status    : UP
 topo index 2   :
      host name      : Transit1
      eips type      : edge
      eips status    : FAULT
      border         : NO
      base MAC       : 0101.7a54.5d71
      sys oid        : 1.3.6.1.4.1.59955.1.102.145
      interface1     : gi0/3
        MAC          : 0101.7a54.5d71
        role         : edge
        block-status   : unblock
        link-status    : UP
Transit2#show eips topology ring 2
 ring ID     : 2
 topo status  : not round
 topo index 1   :
      host name      : sTransit2
      eips type      : transit
      eips status    : FAULT
      border         : NO
```

```
        base MAC       : 2012.1209.1728
        sys oid        : 1.3.6.1.4.1.59955.1.102.126
        interface1     : gi0/1
          MAC          : 2012.1209.1728
          role         : primary
          block-status    : block
          link-status     : DOWN
        interface2     : gi0/2
          MAC          : 2012.1209.1728
          role         : second
          block-status    : unblock
          link-status     : UP
    topo index 2   :
        host name      : Transit2
        eips type      : assistant
        eips status    : FAULT
        border         : NO
        base MAC       : 0101.7a22.2224
        sys oid        : 1.3.6.1.4.1.59955.1.0.0
        interface1     : gi0/3
          MAC          : 0101.7a22.2224
          role         : edge
          block-status    : unblock
          link-status     : UP
Transit1#show eips topology ring 1
 ring ID     : 1
 topo status  : round
 topo index 1   :
        host name      : Transit2
        eips type      : transit
        eips status    : COMPLETE
        border         : YES
        base MAC       : 0101.7a22.2224
        sys oid        : 1.3.6.1.4.1.59955.1.0.0
        interface1     : gi0/1
          MAC          : 0101.7a22.2224
          role         : primary
          block-status    : unblock
          link-status     : UP
        interface2     : gi0/2
          MAC          : 0101.7a22.2224
          role         : second
          block-status    : unblock
          link-status     : UP
    topo index 2   :
```

host name : Transit3
eips type : transit
eips status : COMPLETE
border : NO
base MAC : 0000.0000.008b
sys oid : 1.3.6.1.4.1.59955.1.102.146
interface1 : gi0/1
MAC : 0000.0000.008b
role : primary
block-status : unblock
link-status : UP
interface2 : gi0/2
MAC : 0000.0000.008b
role : second
block-status : unblock
link-status : UP
topo index 3 :
host name : Master
eips type : master
eips status : COMPLETE
border : NO
base MAC : 0014.0000.1202
sys oid : 1.3.6.1.4.1.59955.1.102.127
interface1 : gi0/2
MAC : 0014.0000.1202
role : second
block-status : block
link-status : UP
interface2 : gi0/1
MAC : 0014.0000.1202
role : primary
block-status : unblock
link-status : UP
topo index 4 :
host name : Transit1
eips type : transit
eips status : COMPLETE
border : YES
base MAC : 0101.7a54.5d71
sys oid : 1.3.6.1.4.1.59955.1.102.145
interface1 : gi0/1
MAC : 0101.7a54.5d71
role : primary
block-status : unblock
link-status : UP

```
interface2     : gi0/2
  MAC          : 0101.7a54.5d71
  role         : second
  block-status   : unblock
  link-status    : UP
```

10.3.3.3 Configure EIPS Intersected Rings in the Subring Mode

Network Requirements

- Six devices in the LAN form two-level intersecting rings. Configure the EIPS sub ring mode to block the secondary port gigabitethernet0/2 on Master and secondary port gigabitethernet0/2 on sMaster to achieve the ring protection.
- When the link between Transit1 and Transit2 is disconnected, unblock the STP blocked status for gigabitethernet0/2 on Master of the main ring to achieve data switchover and ensure the communications in Ring1 not affected.
- When the link between sTransit1 and sTransit2 is disconnected, unblock the STP blocked status for gigabitethernet0/2 on sMaster to achieve data switchover and ensure the communications in Ring2 not affected.

Network Topology

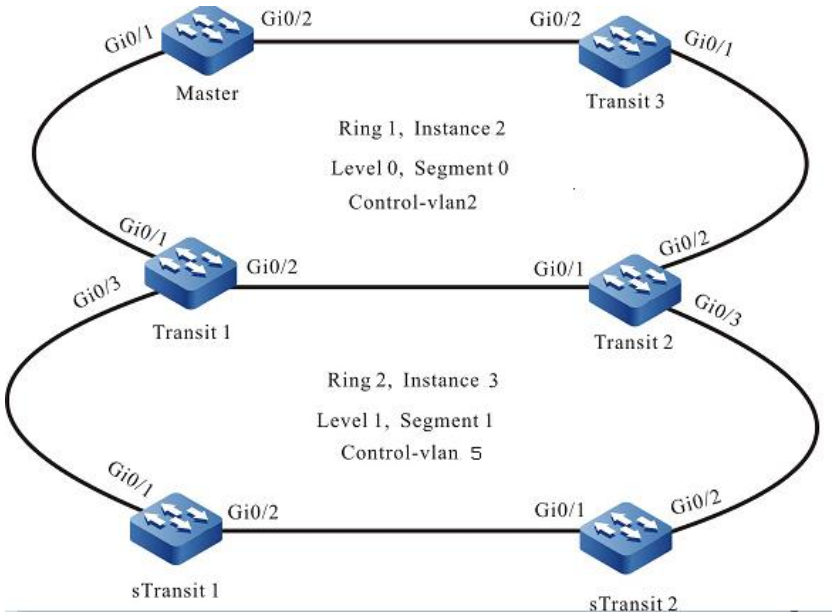


Figure 290 Networking of configuring EIPS intersecting ring in the sub ring mode

Configuration Steps

Step 1: Configure the VLAN and port link type.

#Create VLAN2-VLAN3 on Master. Configure the link type of gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2-VLAN3 to pass. Configure the PVID as 1.

```
Master#configure terminal
Master(config)#vlan 2-4
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#switchport mode trunk
Master(config-if-range)#switchport trunk allowed vlan add 2-3
Master(config-if-range)#switchport trunk pvid vlan 1
```

#Map VLAN2-VLAN3 on Master to the STP instance 2. Disable the STP and storm suppression function on ports gigabitethernet0/1 and gigabitethernet0/2.

```
Master (config)#spanning-tree mst configuration
%Alert: Commands configured under the mode would not take effect immediately, you should active them explicitly!
Master (config-mst)#instance 2 vlan 3
Master (config-mst)#active configuration pending
Master(config-if-range)#exit
Master(config)#interface gigabitethernet 0/1-0/2
Master(config-if-range)#no spanning-tree enable
Master(config-if-range)#no storm-control multicast
Master(config-if-range)#no storm-control unicast
Master(config-if-range)#no storm-control broadcast
Master(config-if-range)#exit
```

#Create vlan2-5 on the master ring transmission node transit1, map vlan3 to spanning tree instance 2, and map vlan4 to spanning tree instance 3. Configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk to allow vlan2-3 services to pass, and configure the link type of ports gigabitethernet0/2-gigabitethernet0/3 as trunk to allow vlan4-5 services to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/3. (omitted)

#Create vlan2-5 on the master ring transmission node transit2, map vlan3 to

spanning tree instance 2, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan2-3 to pass, and configure PVID as 1. Configure the link type of ports gigabitethernet0/2-gigabitethernet0/3 as trunk to allow vlan4-5 services to pass, and configure PVID as 1. Disable spanning tree and storm suppression functions on ports gigabitethernet0/1-gigabitethernet0/3. (omitted)

#Create vlan2 and vlan3 on the master ring transmission node transit3, map vlan3 to spanning tree instance 2, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan2 and vlan3 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

#Create vlan4 and vlan5 on the primary sub ring transmission node sTransit1, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan4 and vlan5 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

#Create vlan4 and vlan5 on the primary sub ring transmission node sTransit2, map vlan4 to spanning tree instance 3, configure the link type of ports gigabitethernet0/1-gigabitethernet0/2 as trunk, allow the traffic of vlan4 and vlan5 to pass, and configure PVID as 1. Disable spanning tree and storm suppression on ports gigabitethernet0/1-gigabitethernet0/2. (omitted)

Note

- VLAN2 is the control VLAN of the master ring, VLAN5 is the control VLAN of the sub ring, which is only used for transmitting EIPs protocol packets, and VLAN 3-4 is the data VLAN, which is used for forwarding services.

- To use the EIPs function, you must map the EIPS data VLAN to the corresponding spanning tree instance, and disable the spanning tree and storm suppression functions on the port.

Step 2: Configure Ring1.

#Create the master node Ring1 in the sub ring mode on Master. Configure the level number of the EIPS ring as 0, domain number as 0, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Master(config)#eips ring 1 master
Master(config-eips)#control vlan 2
Master(config-eips)#level 0
Master(config-eips)#domain id 1
Master(config-eips)#instance 2
Master(config-eips)#primary interface gigabitethernet 0/1
Master(config-eips)#secondary interface gigabitethernet 0/2
Master(config-eips)#eips start
Master(config-eips)#exit
```

#Create the transmission node Ring1 in the sub ring mode on Transit1. Configure the level number of the EIPS ring as 0, domain number as 1, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Transit1(config)#eips ring 1 transit
Transit1(config-eips)#instance 2
Transit1(config-eips)#control vlan 2
Transit1(config-eips)#domain id 1
Transit1(config-eips)#level 0
Transit1(config-eips)#primary interface gigabitethernet0/1
Transit1(config-eips)#secondary interface gigabitethernet0/2
Transit1(config-eips)#eips start
Transit1(config-eips)#exit
```

#Create the transmission node Ring1 in the sub ring mode on Transit2. Configure the level number of the EIPS ring as 0, domain number as 1, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as

gigabitethernet0/2. Enable the EIPS.

```
Transit2(config)#eips ring 1 transit
Transit2(config-eips)#instance 2
Transit2(config-eips)#domain id 1
Transit2(config-eips)#control vlan 2
Transit2(config-eips)#level 0
Transit2(config-eips)#primary interface gigabitethernet0/1
Transit2(config-eips)#secondary interface gigabitethernet0/2
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#Create the transmission node Ring1 in the sub ring mode on Transit3. Configure the level number of the EIPS ring as 0, domain number as 1, instance as 2, control VLAN as VLAN2, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
Transit3(config)#eips ring 1 transit
Transit3(config-eips)#control vlan 2
Transit3(config-eips)#level 0
Transit3(config-eips)#domain id 1
Transit3(config-eips)#instance 2
Transit3(config-eips)#primary interface gigabitethernet 0/1
Transit3(config-eips)#secondary interface gigabitethernet 0/2
Transit3(config-eips)#eips start
Transit3(config-eips)#exit
```

Step 3: Configure Ring2.

#Create the edge node Ring2 in the sub ring mode on Transit1. Configure the level number of the EIPS ring as 0, domain number as 1, instance as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3, and Ring1 as its associated transmission node. Enable the EIPS.

```
Transit1(config)#eips ring 2 edge
Transit1(config-eips)#control vlan 5
Transit1(config-eips)#level 1
Transit1(config-eips)#domain id 1
Transit1(config-eips)#instance 3
Transit1(config-eips)#transit ring 1
Transit1(config-eips)#edge interface gigabitethernet0/3
Transit1(config-eips)#eips start
```

```
Transit1(config-eips)#exit
```

#Create the edge node Ring2 in the sub ring mode on Transit2. Configure the level number of the EIPS ring as 1, domain number as 1, instance as 3, control VLAN as VLAN5, edge port as gigabitethernet0/3, and Ring1 as its associated transmission node. Enable the EIPS.

```
Transit2(config)#eips ring 2 assistant
Transit2(config-eips)#control vlan 5
Transit2(config-eips)#level 1
Transit2(config-eips)#domain id 1
Transit2(config-eips)#instance 3
Transit2(config-eips)#transit ring 1
Transit2(config-eips)#edge interface gigabitethernet0/3
Transit2(config-eips)#eips start
Transit2(config-eips)#exit
```

#Create the master node Ring2 in the sub ring mode on sMaster. Configure the level number of the EIPS ring as 1, the domain of the EIPS ring as 1, the instance of the EIPS ring as 3, control VLAN as VLAN5, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
sMaster(config)#eips ring 2 master
sMaster(config-eips)#level 1
sMaster(config-eips)#domain id 1
sMaster(config-eips)#instance 3
sMaster(config-eips)#control vlan 5
sMaster(config-eips)#primary interface gigabitethernet 0/1
sMaster(config-eips)#secondary interface gigabitethernet 0/2
sMaster(config-eips)#eips start
sMaster(config-eips)#exit
```

Create the transmission node Ring2 in the sub ring mode on sTransit1. Configure the level number of the EIPS ring as 1, domain number as 1, instance as 3, control VLAN as VLAN5, primary port as gigabitethernet0/1, and secondary port as gigabitethernet0/2. Enable the EIPS.

```
sTransit1(config)#eips ring 2 transit
sTransit1(config-eips)#control vlan 5
sTransit1(config-eips)#level 1
sTransit1(config-eips)#domain id 1
sTransit1(config-eips)#instance 3
sTransit1(config-eips)#primary interface gigabitethernet 0/1
```

```
sTransit1(config-eips)#secondary interface gigabitethernet 0/2
sTransit1(config-eips)#eips start
sTransit1(config-eips)#exit
```

Step 4: Check the result.

#Run the **show eips topology-summary** command on the edge node and the edge assistant node. We can view that the EIPS status of the main ring and sub rings is round and the topology information is consistent.

```
Transit1#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1    Transit2       0101.7a22.2224  transit   gi0/1         UP     gi0/2         UP     YES
 2    Transit3       0000.0000.008b  transit   gi0/1         UP     gi0/2         UP     NO
 3    Master         0014.0000.1202  master    gi0/2         UP     gi0/1         UP     NO
 4    Transit1       0101.7a54.5d71  transit   gi0/1         UP     gi0/2         UP     YES

 ring ID     : 2
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1    Transit2       0101.7a22.2224  assistant ----          ----   gi0/3         UP     NO
 2    sTransit1      2012.1209.1728  transit   gi0/2         UP     gi0/1         UP     NO
 3    sMaster        0000.0010.0017  master    gi0/2         UP     gi0/1         UP     NO
 4    Transit1       0101.7a54.5d71  edge      gi0/3         UP     ----          ----   NO

Transit2#show eips topology-summary
 ring ID     : 1
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
 ------------------------------------------------------------------------------------------
---------------------------
 1    Transit3       0000.0000.008b  transit   gi0/1         UP     gi0/2         UP     NO
 2    Master         0014.0000.1202  master    gi0/2         UP     gi0/1         UP     NO
 3    Transit1       0101.7a54.5d71  transit   gi0/1         UP     gi0/2         UP     YES
 4    Transit2       0101.7a22.2224  transit   gi0/1         UP     gi0/2         UP     YES

 ring ID     : 2
 topo status  : round
 seq  host-name      mac         type     interface1      link   interface2      link   isBorder
```

```
-------------------------------------------------------------------------------
---------------------------
1   Transit1      0101.7a54.5d71 edge     ----          ----   gi0/3         UP     NO
2   sMaster       0000.0010.0017 master   gi0/1         UP     gi0/2         UP     NO
3   sTransit1     2012.1209.1728 transit  gi0/1         UP     gi0/2         UP     NO
4   Transit2      0101.7a22.2224 assistant gi0/3        UP     ----          ----   NO
```

#Run the **show eips topology** command on the edge node. We can view that gigabitethernet0/2 on Master and gigabitethernet0/2 on sMaster are blocked and the other ports are unblocked. The EIPS status of Master on the main ring and sMaster on the sub ring is COMPLETE and the EIPS status of the other ports is LINK-UP.

```
Transit1#show eips topology
 ring ID     : 1
 topo status  : round
 topo index 1   :
      host name      : Transit2
      eips type      : transit
      eips status    : LINK-UP
      border         : YES
      base MAC       : 0101.7a22.2224
      sys oid        : 1.3.6.1.4.1.59955.1.0.0
      interface1     : gi0/1
        MAC          : 0101.7a22.2224
        role         : primary
        block-status   : unblock
        link-status    : UP
      interface2     : gi0/2
        MAC          : 0101.7a22.2224
        role         : second
        block-status   : unblock
        link-status    : UP
 topo index 2   :
      host name      : Transit3
      eips type      : transit
      eips status    : LINK-UP
      border         : NO
      base MAC       : 0000.0000.008b
      sys oid        : 1.3.6.1.4.1.59955.1.102.146
      interface1     : gi0/1
        MAC          : 0000.0000.008b
        role         : primary
        block-status   : unblock
        link-status    : UP
      interface2     : gi0/2
```

```
        MAC          : 0000.0000.008b
        role         : second
        block-status   : unblock
        link-status    : UP
    topo index 3   :
      host name      : Master
      eips type      : master
      eips status    : COMPLETE
      border         : NO
      base MAC       : 0014.0000.1202
      sys oid        : 1.3.6.1.4.1.59955.1.102.127
      interface1     : gi0/2
        MAC          : 0014.0000.1202
        role         : second
        block-status   : block
        link-status    : UP
      interface2     : gi0/1
        MAC          : 0014.0000.1202
        role         : primary
        block-status   : unblock
        link-status    : UP
    topo index 4   :
      host name      : Transit1
      eips type      : transit
      eips status    : LINK-UP
      border         : YES
      base MAC       : 0101.7a54.5d71
      sys oid        : 1.3.6.1.4.1.59955.1.102.145
      interface1     : gi0/1
        MAC          : 0101.7a54.5d71
        role         : primary
        block-status   : unblock
        link-status    : UP
      interface2     : gi0/2
        MAC          : 0101.7a54.5d71
        role         : second
        block-status   : unblock
        link-status    : UP

    ring ID     : 2
    topo status  : round
    topo index 1   :
      host name      : Transit2
      eips type      : assistant
      eips status    : LINK-UP
```

```
        border        : NO
        base MAC      : 0101.7a22.2224
        sys oid       : 1.3.6.1.4.1.59955.1.0.0
        interface2    : gi0/3
          MAC         : 0101.7a22.2224
          role        : edge
          block-status  : unblock
          link-status   : UP
    topo index 2  :
        host name     : sTransit1
        eips type     : transit
        eips status   : LINK-UP
        border        : NO
        base MAC      : 2012.1209.1728
        sys oid       : 1.3.6.1.4.1.59955.1.102.126
        interface1    : gi0/2
          MAC         : 2012.1209.1728
          role        : second
          block-status  : unblock
          link-status   : UP
        interface2    : gi0/1
          MAC         : 2012.1209.1728
          role        : primary
          block-status  : unblock
          link-status   : UP
    topo index 3  :
        host name     : sMaster
        eips type     : master
        eips status   : COMPLETE
        border        : NO
        base MAC      : 0000.0010.0017
        sys oid       : 1.3.6.1.4.1.59955.1.102.140
        interface1    : gi0/2
          MAC         : 0000.0010.0017
          role        : second
          block-status  : block
          link-status   : UP
        interface2    : gi0/1
          MAC         : 0000.0010.0017
          role        : primary
          block-status  : unblock
          link-status   : UP
    topo index 4  :
        host name     : Transit1
        eips type     : edge
```

```
    eips status     : LINK-UP
    border          : NO
    base MAC        : 0101.7a54.5d71
    sys oid         : 1.3.6.1.4.1.59955.1.102.145
    interface1      : gi0/3
      MAC           : 0101.7a54.5d71
      role          : edge
      block-status    : unblock
      link-status     : UP
```

#When the link between Transit1 and Transit2 is disconnected, run the **show eips topology** command on the edge node again. We can view that the status of Ring1 changes to not round and the EIPS status of Transit1 and Transit2 changes to LINK-DOWN. The EIPS status of Master on the main ring changes to FAULT and gigabitethernet0/2 on Master changes to unblock. Transit1 communicates with Transit2 via Master, which ensures uninterrupted communications between Transit1 and Transit2. The status of Ring2 is still round, the EIPS status of sMaster is still COMPLETE, and gigabitethernet0/2 of sMaster is still blocked.

```
Transit1#show eips topology ring 1
 ring ID     : 1
 topo status  : not round
 topo index 1  :
      host name       : Transit2
      eips type       : transit
      eips status     : LINK-DOWN
      border          : YES
      base MAC        : 0101.7a22.2224
      sys oid         : 1.3.6.1.4.1.59955.1.0.0
      interface1      : gi0/1
        MAC           : 0101.7a22.2224
        role          : primary
        block-status    : block
        link-status     : DOWN
      interface2      : gi0/2
        MAC           : 0101.7a22.2224
        role          : second
        block-status    : unblock
        link-status     : UP
 topo index 2  :
      host name       : Transit3
      eips type       : transit
```

```
        eips status     : LINK-UP
        border          : NO
        base MAC        : 0000.0000.008b
        sys oid         : 1.3.6.1.4.1.59955.1.102.146
        interface1      : gi0/1
          MAC           : 0000.0000.008b
          role          : primary
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/2
          MAC           : 0000.0000.008b
          role          : second
          block-status    : unblock
          link-status     : UP
    topo index 3   :
        host name       : Master
        eips type       : master
        eips status     : FAULT
        border          : NO
        base MAC        : 0014.0000.1202
        sys oid         : 1.3.6.1.4.1.59955.1.102.127
        interface1      : gi0/2
          MAC           : 0014.0000.1202
          role          : second
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/1
          MAC           : 0014.0000.1202
          role          : primary
          block-status    : unblock
          link-status     : UP
    topo index 4   :
        host name       : Transit1
        eips type       : transit
        eips status     : LINK-DOWN
        border          : YES
        base MAC        : 0101.7a54.5d71
        sys oid         : 1.3.6.1.4.1.59955.1.102.145
        interface1      : gi0/1
          MAC           : 0101.7a54.5d71
          role          : primary
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/2
          MAC           : 0101.7a54.5d71
```

```
        role          : second
        block-status    : block
        link-status     : DOWN

Transit1#show eips topology ring 2
 ring ID     : 2
 topo status  : round
 topo index 1   :
      host name      : Transit2
      eips type      : assistant
      eips status     : LINK-UP
      border         : NO
      base MAC       : 0101.7a22.2224
      sys oid        : 1.3.6.1.4.1.59955.1.0.0
      interface2     : gi0/3
        MAC          : 0101.7a22.2224
        role         : edge
        block-status    : unblock
        link-status     : UP
 topo index 2   :
      host name      : sTransit1
      eips type      : transit
      eips status     : LINK-UP
      border         : NO
      base MAC       : 2012.1209.1728
      sys oid        : 1.3.6.1.4.1.59955.1.102.126
      interface1     : gi0/2
        MAC          : 2012.1209.1728
        role         : second
        block-status    : unblock
        link-status     : UP
      interface2     : gi0/1
        MAC          : 2012.1209.1728
        role         : primary
        block-status    : unblock
        link-status     : UP
 topo index 3   :
      host name      : sMaster
      eips type      : master
      eips status     : COMPLETE
      border         : NO
      base MAC       : 0000.0010.0017
      sys oid        : 1.3.6.1.4.1.59955.1.102.140
      interface1     : gi0/2
        MAC          : 0000.0010.0017
```

```
    role          : second
    block-status    : block
    link-status     : UP
  interface2      : gi0/1
    MAC           : 0000.0010.0017
    role          : primary
    block-status    : unblock
    link-status     : UP
topo index 4   :
  host name       : Transit1
  eips type       : edge
  eips status     : LINK-UP
  border          : NO
  base MAC        : 0101.7a54.5d71
  sys oid         : 1.3.6.1.4.1.59955.1.102.145
  interface1      : gi0/3
    MAC           : 0101.7a54.5d71
    role          : edge
    block-status    : unblock
    link-status     : UP
```

#When only the link between sTransit1 and Transit2 is disconnected, run the **show eips topology** command again on Transit1 and Transit2. We can view that the status of Ring2 changes to not round, the EIPS status of sMaster changes to FAULT, and gigabitethernet0/2 of sMaster changes to unblock. sTransit1 communicates with Transit2 via sMaster, which ensures uninterrupted communications between sTransit1 and Transit2. The status of Ring1 is still round, the EIPS status is still COMPLETE, and gigabitethernet0/2 on Master is still blocked.

```
Transit1#show eips topology ring 2
 ring ID      : 2
 topo status  : not round
 topo index 1   :
   host name       : sTransit1
   eips type       : transit
   eips status     : LINK-DOWN
   border          : NO
   base MAC        : 2012.1209.1728
   sys oid         : 1.3.6.1.4.1.59955.1.102.126
   interface1      : gi0/2
     MAC           : 2012.1209.1728
     role          : second
     block-status    : block
```

```
        link-status     : DOWN
      interface2      : gi0/1
        MAC           : 2012.1209.1728
        role          : primary
        block-status    : unblock
        link-status     : UP
topo index 2   :
      host name       : sMaster
      eips type       : master
      eips status     : FAULT
      border          : NO
      base MAC        : 0000.0010.0017
      sys oid         : 1.3.6.1.4.1.59955.1.102.140
      interface1      : gi0/2
        MAC           : 0000.0010.0017
        role          : second
        block-status    : unblock
        link-status     : UP
      interface2      : gi0/1
        MAC           : 0000.0010.0017
        role          : primary
        block-status    : unblock
        link-status     : UP
topo index 3   :
      host name       : Transit1
      eips type       : edge
      eips status     : LINK-UP
      border          : NO
      base MAC        : 0101.7a54.5d71
      sys oid         : 1.3.6.1.4.1.59955.1.102.145
      interface1      : gi0/3
        MAC           : 0101.7a54.5d71
        role          : edge
        block-status    : unblock
        link-status     : UP
Transit2#show eips topology ring 2
 ring ID      : 2
 topo status  : not round
 topo index 1   :
      host name       : Transit2
      eips type       : assistant
      eips status     : LINK-DOWN
      border          : NO
      base MAC        : 0101.7a22.2224
      sys oid         : 1.3.6.1.4.1.59955.1.0.0
```

```
        interface1      : gi0/3
          MAC           : 0101.7a22.2224
          role          : edge
          block-status    : block
          link-status     : DOWN
Transit1#show eips topology ring 1
 ring ID      : 1
 topo status  : round
 topo index 1   :
        host name       : Transit2
        eips type       : transit
        eips status     : LINK-UP
        border          : YES
        base MAC        : 0101.7a22.2224
        sys oid         : 1.3.6.1.4.1.59955.1.0.0
        interface1      : gi0/1
          MAC           : 0101.7a22.2224
          role          : primary
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/2
          MAC           : 0101.7a22.2224
          role          : second
          block-status    : unblock
          link-status     : UP
 topo index 2   :
        host name       : Transit3
        eips type       : transit
        eips status     : LINK-UP
        border          : NO
        base MAC        : 0000.0000.008b
        sys oid         : 1.3.6.1.4.1.59955.1.102.146
        interface1      : gi0/1
          MAC           : 0000.0000.008b
          role          : primary
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/2
          MAC           : 0000.0000.008b
          role          : second
          block-status    : unblock
          link-status     : UP
 topo index 3   :
        host name       : Master
        eips type       : master
```

```
        eips status     : COMPLETE
        border          : NO
        base MAC        : 0014.0000.1202
        sys oid         : 1.3.6.1.4.1.59955.1.102.127
        interface1      : gi0/2
          MAC           : 0014.0000.1202
          role          : second
          block-status    : block
          link-status     : UP
        interface2      : gi0/1
          MAC           : 0014.0000.1202
          role          : primary
          block-status    : unblock
          link-status     : UP
    topo index 4   :
        host name       : Transit1
        eips type       : transit
        eips status     : LINK-UP
        border          : YES
        base MAC        : 0101.7a54.5d71
        sys oid         : 1.3.6.1.4.1.59955.1.102.145
        interface1      : gi0/1
          MAC           : 0101.7a54.5d71
          role          : primary
          block-status    : unblock
          link-status     : UP
        interface2      : gi0/2
          MAC           : 0101.7a54.5d71
          role          : second
          block-status    : unblock
          link-status     : UPULPP and Monitor Link
```

10.4 link-status : UPULPP and Monitor Link

10.4.1 Overview

The dual-uplink networking mode is one common networking mode of the core network. The networking mode improves the network reliability via the redundant link. The common solution of removing the redundant link is to use STP, but the convergence time of STP cannot meet the carrier-class Ethernet requirement. In this case, ULPP (Uplink Protect Protocol) comes into being.

ULPP meets the performance requirement of the user for the link fast convergence

and realizes the redundant backup of the active/standby link and the fast switchover of the traffic, but also simplifies the configuration efficiently. This makes the deployment and maintenance become more convenient and improves the work efficiency of the deploying and maintaining staff.

Monitor Link provides one linkage management technology of the link status change. The ports in the Monitor Link group include one uplink port and multiple downlink ports. The uplink port is monitored in real time. When the uplink port status changes, set the downlink ports at the same time, so as to synchronously inform the uplink device port status to the downlink device fast. This is helpful for STP and ULPP modules to respond the network change and switch the traffic.

10.4.2 ULPP Function Configuration

Table 1317 ULPP function configuration list

Configuration Task	
Configure the ULPP basic functions	Configure the ULPP group
	Configure the ULPP uplink port
Configure the ULPP compatible mode	Configure the compatible mode of the ULPP group
	Configure the compatible mode of the ULPP uplink port
Configure the Monitor Link basic function	Configure the Monitor Link group

10.4.2.1 Configure ULPP Basic Functions

Configuration Condition

Before configuring the ULPP basic function, first complete the following task:

- Configure the spanning tree instance mapping of the ULPP group
- When configuring the control VLAN of the ULPP group, it is required that the VLAN is created
- The member port of the ULPP group should be added to the control VLAN

Configure ULPP Group

The ULPP group contains two ports, that is, master port and slave port. The ULPP group has two work modes, that is, the link backup and load balance. In the link backup mode, only one of the master or slave port of the ULPP group is in the forwarding state; the other is blocked and in the standby state. When the normal forwarding port link fails, the ULPP group automatically blocks the port and switches the blocked standby port to the forwarding state. In the load balance mechanism, the ULPP group bears the spanning tree instance traffic in different VLANs according to the binding relation of the spanning tree instance and port configured on the master/slave port.

Table 1318 Configure the ULPP group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the ULPP group and enter the ULPP configuration mode	ulpp-group *group-id*	Mandatory By default, do not create the ULPP group.
Configure the master port of ULPP	master { interface *interface-name* | link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the master port of the ULPP group.
Configure the slave port of the ULPP group	slave { interface *interface-name* | link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the slave port of the ULPP group.
Configure the instance of the ULPP group	instance group *instance-number* { master | slave }	Mandatory By default, do not configure the instance of the ULPP group. The spanning tree instances of the master port and slave port cannot intersect.
Configure the control	control-vlan *vlan-id*	Mandatory

Step	Command	Description
VLAN of the ULPP group		By default, do not configure the control VLAN of the ULPP group.
Configure enabling the ULPP group	enable	Mandatory By default, do not configure enabling the ULPP group
Enable the function of the ULPP sending the FLUSH packet	flush enable	Optional By default, do not enable the function of the ULPP group sending the FLUSH packet
Configure the work mode of the ULPP group	mode { load-balance | backup }	Optional By default, the ULPP group is the master/slave (backup) mode.
Configure the role preemption function of the ULPP group	preemption mode role	Optional By default, do not configure the ULPP group role preemption. When the work mode of the ULPP group is the link backup mode, the role preemption function can be configured.

Note

- The member port of the ULPP group should disable the EIPS, STP and loopback detection function.
- The member port of the ULPP group cannot be the member port of the ULPP group and Monitor Link group.
- The control VLAN of the ULPP group cannot be used to forward the

service data.

- One ULPP group can only have one control VLAN; one control VLAN can only belong to one ULPP group.
- After disabling the ULPP group, the member ports are all blocked in all spanning tree instances.

Configure ULPP Uplink Port

When the link switching happens to the ULPP group, the ULPP group sends the FLUSH packets to inform other devices to refresh the address table, so as to ensure the fast switching of the service traffic in the network. The uplink port not only receives the FLUSH packet, but also forwards the FLUSH packet in the control VLAN of the device.

Table 1319 Configure the uplink port control VLAN of the ULPP group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the port 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 uplink port control VLAN of the ULPP group	ulpp flush control-vlan *vlan-list*	Mandatory By default, do not configure the uplink port control VLAN of the ULPP group

10.4.2.2 Configure ULPP Compatible Mode

Configuration Condition

Before configuring the ULPP compatible mode, first complete the following tasks:

- To configure the ULPP group compatible mode, we need to configure the basic functions of the ULPP group
- To configure the ULPP uplink port compatible mode, we need to configure the ULPP uplink port control VLAN first

Configure ULPP Group Compatible Mode

The ULPP group can be compatible with three modes, that is, flexlink, smartlink, and smartlink multicast-mode.

Table 1320 Configure the ULPP group compatible mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ULPP configuration mode	ulpp-group *group-id*	-
Configure the ULPP group compatible mode	compatible { flexlink | smartlink | smartlink multicast-mode }	Mandatory By default, do not configure the ULPP group compatible mode

Configure ULPP Uplink Port Compatible Mode

The ULPP uplink port can be compatible with three modes, that is, flexlink, smartlink, and smartlink multicast-mode.

Table 1321 Configure the ULPP uplink port compatible 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 ULPP uplink port compatible mode	ulpp compatible { flexlink | smartlink | smartlink multicast-mode }	Mandatory By default, do not configure the ULPP group uplink port compatible mode.

Note

- The ULPP group uplink port can configure the compatible mode only after disabling the spanning tree.

10.4.2.3 Configure Basic Functions of Monitor Link Group

Configuration Condition

None

Configure Monitor Link Group

The monitor link group can have multiple uplink ports, which can be ordinary ports, aggregation group member ports, aggregation groups, VSL ports or ULDP groups. The monitor link group can have multiple downlink ports, which can be

ordinary ports, aggregation group member ports and aggregation groups, not ULDP groups.

Table 1322 Configure the Monitor Link group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the Monitor Link group and enter the Monitor Link configuration mode	mtlk-group *group-id*	Mandatory By default, do not create the Monitor Link group.
Configure the uplink port of the Monitor Link group	uplink { interface *interface-name* | link-aggregation *link-aggregation-id* | ulpp-group *group-id* }	Optional By default, do not configure the uplink port of the Monitor Link group.
Configure the downlink port of the Monitor Link group	downlink { interface *interface-name* | link-aggregation *link-aggregation-id* }	Optional By default, do not configure the downlink port of the Monitor Link group.
Configure the delay UP time of the Monitor Link group downlink port	Downlink up-delay *time*	Optional By default, the delay UP time of the downlink port is 0.
Configure the threshold value of the Monitor Link group uplink port	uplink up-port-threshold *number*	Optional By default, the threshold of the uplink port is 1.

10.4.2.4 ULPP Monitoring and Maintaining

Table 1323 ULPP monitoring and maintaining

Command	Description
clear ulpp message flush { receive | send group *group-id* | transmit }	Clear the statistics information of the FLUSH packets of the ULPP group
show ulpp group *group-id*	Display the ULPP group configuration information
show ulpp instance group *group-id*	Display the spanning tree status born by the master/standby member port of the ULPP group
show ulpp message flush { send group *group-id* |	Display the statistics information of the FLUSH

Command	Description
receive | transmit }	packets processed by the ULPP group
show ulpp assi	Display the configuration information of the ULPP group uplink port
show mtlk group *group-id*	Display the configuration information of the Monitor Link group

10.4.3 Typical Configuration Example of ULPP and Monitor Link

10.4.3.1 Configure ULPP

Network Requirements

- Four devices form the dual-uplink networking. The uplink devices are Device1, Device2, and Device3; the downlink device is Device4.
- Configure the ULPP function on the downlink device so that the port normally bears or switches the services in the associated spanning tree instance.

Network Topology

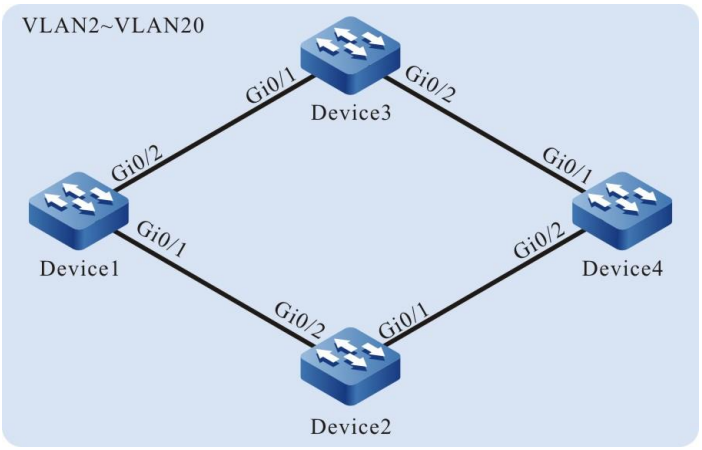


Figure 291 Networking of configuring the ULPP group

Configuration Steps

Step 1: Configure the link type of the VLAN and port.

#Create VLAN2-VLAN20 on Device1, configure the link type of port gigabiteternet0/1, gigabiteternet0/2 on Device1 as Trunk; permit the services of VLAN2-VLAN20 to pass.

```
Device1#configure terminal
Device1(config)#vlan 2-20
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/2)#exit
```

Note

- The configuration of the VLAN, port and link type of Device2, Device3, and Device4 is the same as that of Device1. (Omitted)

Step 2: Configure the spanning tree instance on Device4.

#Configure the spanning tree instance; instance 1 maps VLAN3-VLAN10; instance 2 maps VLAN11-VLAN20.

```
Device4(config)#spanning-tree mst configuration
Device4(config-mst)#region-name admin
Device4(config-mst)#revision-level 1
Device4(config-mst)#instance 1 vlan 3-10
Device4(config-mst)#instance 2 vlan 11-20
```

#Enable the spanning tree instance.

```
Device4(config-mst)#active configuration pending
Device4(config-mst)#exit
```

Step 3: Configure the ULPP function on Device4.

#Create the ULPP group.

```
Device4(config)#ulpp-group 1
```

#Configure the master port gigabitethernet0/1 and slave port gigabitethernet0/2 of the ULPP group.

```
Device4(config-ulpp-1)#master interface gigabitethernet 0/1
Device4(config-ulpp-1)#slave interface gigabitethernet 0/2
```

#Configure the master port gigabitethernet0/1 to link with the spanning tree instance 1 and slave port gigabitethernet0/2 to link with the spanning tree instance 2.

```
Device4(config-ulpp-1)#instance group 1 master
Device4(config-ulpp-1)#instance group 2 slave
```

#Configure the work mode of the ULPP group as the link backup.

```
Device4(config-ulpp-1)#mode backup
```

#Configure the control VLAN of the ULPP group as VLAN2.

```
Device4(config-ulpp-1)#control-vlan 2
```

#Enable the sending mechanism of the ULPP Flush packet.

```
Device4(config-ulpp-1)#flush enable
```

#Enable the ULPP group.

```
Device4(config-ulpp-1)#enable
Device4(config-ulpp-1)#exit
```

Note

- After VLAN2 is configured as control VLAN, only the Flush packets can pass in the VLAN, but the other service packets cannot.

Step 4: Configure the uplink device Device1, Device2 and Device3.

#Configure the receiving and sending mechanism of the Flush packets on Device1.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#ulpp flush control-vlan 2
Device1(config-if-range)#exit
```

Note

- The receiving and forwarding mechanism of Device2 and Device3 is the same as that of Device1. (Omitted)

Step 5: Check the result.

#View the ULPP group status on Device4.

```
Device4#show ulpp group 1
-------------------------------------
ulpp-group 1 configuration information
-------------------------------------
Current status          : MASS
Work type               : Backup
Control vlan            : 2
Flush function          : Enable
Preemtion mode          : Disable
Master interface name       : gi0/1
Slave interface name        : gi0/2
Master interface status     : Active
Slave interface status      : Standby
Master interface instance   : 1
Slave interface instance    : 2
Flexlink compatible         : Disable
Smartlink compatible        : Disable
Smartlink mcast compatible  : Disable
Enable status           : Enable
```

#View the status of the associated spanning tree instance of the master and slave port on Device4.

```
Device4#show ulpp instance group 1
-------------------------------------
ulpp-group 1 instance status
-------------------------------------
Master forwarding instance  : 1-2
Master block instance       : None
Slave  forwarding instance  : None
Slave  block instance       : 1-2
```

#After port gigabitethernet0/1 of Device4 fails, switch over the status of the ULPP

group. View the status of the ULPP group on Device4.

```
Device4#show ulpp group 1
-------------------------------------
ulpp-group 1 configuration information
-------------------------------------
Current status              : MNSA
Work type                   : Backup
Control vlan                : 2
Flush function              : Enable
Preemtion mode              : Disable
Master interface name       : gi0/1
Slave interface name        : gi0/2
Master interface status     : Down
Slave interface status      : Active
Master interface instance   : 1
Slave interface instance    : 2
Flexlink compatible         : Disable
Smartlink compatible        : Disable
Smartlink mcast compatible  : Disable
Enable status               : Enable
```

The master port gigabitethernet0/1 changes from Active to Down; the slave port gigabitethernet0/2 changes from Standby to Active; the services in the spanning tree instance are forwarded normally via gigabitethernet0/2.

#The uplink device Device1 and Device2 prints the following information.

```
19:26:10: [tUlpp]%ULPP-ASSI: Receive flush message from gigabitethernet0/2 success, the receive sequence number is 1, vlan id is 2
```

The printed is the information of the Flush packet received by the uplink device Device1 and Device2 when the status of the ULPP group switches.

10.4.3.2 Configure Monitor Link

Network Requirements

- Four devices form the dual-uplink networking. The uplink devices are Device1, Device2, and Device3; the downlink device is Device4.
- Configure the Monitor Link function on Device3, realizing the monitoring of the link fault.
- When the uplink port of the Monitor Link group fails, disable the downlink

port, causing the master/slave link switchover of the ULPP group and ensuring the connectivity of the network.

Network Topology

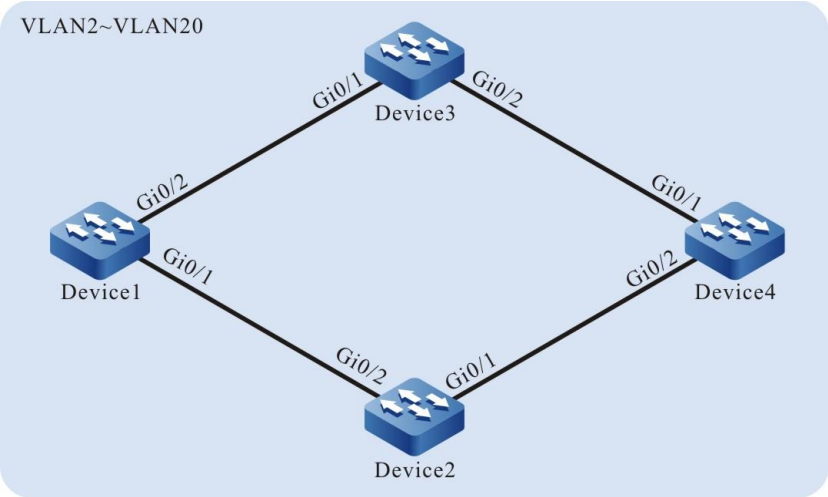


Figure 292 Networking of configuring Monitor Link

Configuration Steps

Step 1: Configure the link type of the VLAN and port.

#Create VLAN2-VLAN20 on Device1, configure the link type of port gigabiteternet0/1, gigabiteternet0/2 on Device1 as Trunk; permit the services of VLAN2-VLAN20 to pass.

```
Device1#configure terminal
Device1(config)#vlan 2-20
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)#switchport mode trunk
Device1(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2-20
Device1(config-if-gigabitethernet0/2)#exit
```

Note

- The configuration of the port and link type of Device2, Device3, and Device4 is the same as that of Device1. (Omitted)

Step 2: Configure the spanning tree instance on Device4.

#Configure the spanning tree instance; instance 1 maps VLAN3-VLAN10; instance 2 maps VLAN11-VLAN20.

```
Device4(config)#spanning-tree mst configuration
Device4(config-mst)#region-name admin
Device4(config-mst)#revision-level 1
Device4(config-mst)#instance 1 vlan 3-10
Device4(config-mst)#instance 2 vlan 11-20
```

#Enable the spanning tree instance.

```
Device4(config-mst)#active configuration pending
Device4(config-mst)#exit
```

Step 3: Configure the ULPP function on Device4.

```
Device4(config)#ulpp-group 1
Device4(config-ulpp-1)#master interface gigabitethernet 0/1
Device4(config-ulpp-1)#slave interface gigabitethernet 0/2
Device4(config-ulpp-1)#instance group 1 master
Device4(config-ulpp-1)#instance group 2 slave
Device4(config-ulpp-1)#mode backup
Device4(config-ulpp-1)#control-vlan 2
Device4(config-ulpp-1)#flush enable
Device4(config-ulpp-1)#enable
Device4(config-ulpp-1)#exit
```

Note

- After VLAN2 is configured as control VLAN, only the Flush packets can pass in the VLAN, but the other service packets cannot.

Step 4: Configure the uplink device Device1, Device2 and Device3.

#Configure the receiving and sending mechanism of the Flush packets on Device1.

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#ulpp flush control-vlan 2
Device1(config-if-range)#exit
```

Note

- The receiving and forwarding mechanism of Device2 and Device3 is the same as that of Device1. (Omitted)

Step 5: Configure the Monitor Link group.

#Create the Monitor Link group on Device3.

```
Device3(config)#mtlk-group 1
```

#Configure gigabitethernet0/1 as the uplink port of the Monitor Link group on Device3.

```
Device3(config-mtlk-1)#uplink interface gigabitethernet 0/1
```

#Configure gigabitethernet0/2 as the downlink port of the Monitor Link group on Device3.

```
Device3(config-mtlk-1)#downlink interface gigabitethernet 0/2
```

#View the Monitor Link group.

```
Device3#show mtlk group 1
--------------------------------------
mtlk-group 1 configuration information
--------------------------------------
Uplink interface        : gi0/1
Uplink type             : no-ulpp
Uplink status           : up
Downlink interface      : gi0/2
```

Step 6: Check the result.

#After the uplink port gigabitethernet0/1 of the uplink device Device3 fails, the status of the downlink port gigabitethernet0/2 keeps linkage with the status of the uplink port gigabitethernet0/1. The downlink port is forced to be disabled.

#View the status of the downlink port gigabitethernet0/2.

```
Device3#show interface gigabitethernet 0/2
gigabitethernet0/2 configuration information
    Description     : downlink
    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     : 0101.7a58.000b
```

The downlink port gigabitethernet0/2 is disabled, causing the master/slave link switchover of the ULPP group of Device4 and ensuring the connectivity of the network.

10.5 VRRP

10.5.1 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”.

10.5.2 VRRP Function Configuration

Table 1324 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
Configure VRRP delay degradation	Configure the VRRP delay degradation
Configure the VRRP packet disperse	Configure VRRP packet disperse
Configure VRRP delat restore	Configure the VRRP delay restore
Configure VRRP virtual MAC dual-wielding	Configure VRRP virtual MAC dual-wielding
Configure the static VRRP function	Configure the static VRRP function
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

10.5.2.1 Configure VRRP Basic Functions

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 Condition

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 1325 Enable the VRRP protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the VRRP group	vrrp *vrid* ip *ip-address*	Mandatory Enable the VRRP protocol. The vrid is the VRRP group number. 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 1326 Configure the VRRP priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
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 remains unchanged. If the user really needs to configure the virtual IP address to be 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 1327 Configure the VRRP preemption mode

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

Step	Command	Description
Configure the VRRP group as the preemption mode	vrrp *vrid* preempt [delay *delay-time*]	Mandatory By default, enable the preemption mode, and the preemption delay time is 0ms.

Note

- When the preemption delay time is the default value, the preemption time is 3 times of the packet interval plus the delay time.
- When the preemption delay time is not the default value, the preemption time is the preemption delay time plus the delay time.

Configure Real MAC Address of VRRP

One virtual router 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 router 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 1328 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*	-
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 of this section, use the real MAC, that is, when the host sends the packet, forward by the real MAC address; after deleting the command of this section, use the virtual MAC address, that is, when the host sends the packet, use the virtual MAC address to forward.

10.5.2.2 Configure VRRP Link Group

VRRP linkage group can reduce the interaction of VRRP protocol packets, reduce the network load, and achieve millisecond switching. By adding multiple ordinary VRRP groups to one VRRP linkage group, different VRRP groups play different roles in the linkage group, such as active or non-active. The active group in the linkage group sends protocol packets instead of the non-active group. The state of the non-active group is consistent with that of the active group, that is, the state of the active group is switched, and the state of the non active group will also be switched at the same time, so as to achieve the purpose of reducing protocol packet interaction. Moreover, the linkage group can configure the sending period of VRRP packets to milliseconds, so as to achieve the purpose of fast switching.

Configuration Condition

Before configuring the VRRP link group, first complete the following task:

- Configure multiple VRRP groups

Configure VRRP Link Group

To configure the VRRP link group, first create one VRRP link group and then add the configured common VRRP group to the created link group. When the common VRRP group is added to the link group, it can be added in the Active or non-Active group form, but one link group should have one Active group and can only have one Active group.

Table 1329 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 *lrid* [active]	Mandatory If not selecting active, add by the 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.

10.5.2.3 Configure VRRP Network Authentication

VRRP supports the simple text authentication. The set length of the text authentication cannot 8-bit authentication word.

Configuration Condition

Before configuring the VRRP network authentication, first complete the following task:

- Configure one VRRP group

Configure VRRP Simple Text Authentication

Table 1330 Configure the VRRP simple text authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
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 up to eight characters.

10.5.2.4 Configure VRRP Delay Degradation

In order to meet the requirements of high reliability scenarios, VRRP can configure the delay degradation function. When the device state of VRRP is switched from master to backup, it can still undertake the forwarding of service traffic within the delay degradation time, so as to effectively prevent the loss of service traffic caused by the slow switching of downstream switching device traffic. However, backup devices that are still in delay degradation can forward traffic whose destination MAC address is a virtual MAC address. Therefore, in the stage that the delay degradation timer takes effect, the backup device will also forward traffic packets, resulting in the problem of sending up double traffic. It is recommended not to use this function in scenarios where the reliability requirements are not very high, so as to prevent the impact of double traffic on the network.

Configuration Condition

Before configuring the VRRP delay degradation function, first complete the

following task:

- Configure one VRRP group

Configure VRRP Delay Degradation

Table 1331 Configure VRRP delay degradation

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure VRRP delay degradation	vrrp *vrid* degrade-delay *delay-time*	Mandatory Configure VRRP delay degradation. Here, vrid is the VRRP group number, and delay-time is the delay degradation time.

10.5.2.5 Configure VRRP Packet Disperse

In order to meet the requirements of high reliability scenarios, the VRRP packet disperse function can be configured in the scenario of configuring a large number of VRRP groups. When VRRP bursts, the sending time of VRRP packets can be dispersed to ensure the balanced sending of VRRP packets.

Configuration Condition

None

Configure VRRP Packet Disperse

Table 1332 Configure VRRP packet disperse

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Configure VRRP packet disperse	vrrp disperse- skew *skew-time*	Mandatory Configure VRRP packet disperse. Here, skew-time is the disperse interval of the packet.

10.5.2.6 Configure VRRP Delay Restore

In order to meet the requirements of high reliability scenarios, VRRP delay recovery function can be configured. When the interface state of the VRRP device is switched from down to up, VRRP will wait for the delay recovery time in the INIT state before switching the state.

Configuration Condition

Before configuring the VRRP delay restore function, first complete the following task:

- Configure one VRRP group

Configure VRRP Delay Restore

Table 1333 Configure VRRP delay restore

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure VRRP delay restore	vrrp restore-delay *delay-time*	Mandatory Configure the VRRP delay restore, Here, delay-time is the VRRP restore delay time.

10.5.2.7 Configure VRRP Virtual MAC Dual-Wielding

In order to meet the requirements of high reliability scenarios, the VRRP virtual MAC dual wielding function can be configured. When the master fails and the VRRP device state has not been switched from backup to master, the backup device can quickly take over the forwarding of service traffic and effectively shorten the gateway black hole time. However, in normal usage scenarios, if the downstream switch device

has a flood of traffic, it will cause the backup device that enables MAC dual wielding to also forward traffic packets, resulting in the problem of sending up dual traffic. It is recommended not to use this function in scenarios where the reliability requirements are not very high, so as to prevent the impact of double traffic on the network.

Configuration Conditions

Before configuring the VRRP delay restore function, first complete the following task:

- Configure one VRRP group
- The VRRP group uses the virtual MAC address

Configure VRRP Virtual MAC Dual-Wielding

Table 1334 Configure VRRP virtual MAC dual-wielding

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure VRRP virtual MAC dual-wielding	vrrp *vrid* svlm	Mandatory Configure VRRP virtual MAC dual-wielding. Here, vrid is the VRRP group number.

10.5.2.8 Configure Static VRRP Function

After the static VRRP function is enabled, VRRP does not perform protocol interaction, and the state will eventually remain in the master. The ARP response can be performed normally. It is suitable for single device virtual gateway and MLAG scenarios

Configuration Conditions

Before configuring the static VRRP function, first complete the following task:

- Configure one VRRP group

Configure Static VRRP Function

Table 1335 Configure static VRRP

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure static VRRP	vrrp *vrid* static	Mandatory Configure the static VRRP. Here, vrid is the VRRP group number.

10.5.2.9 Configure VRRP to Link with Track

VRRP can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRP reliability.

Configuration Condition

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.

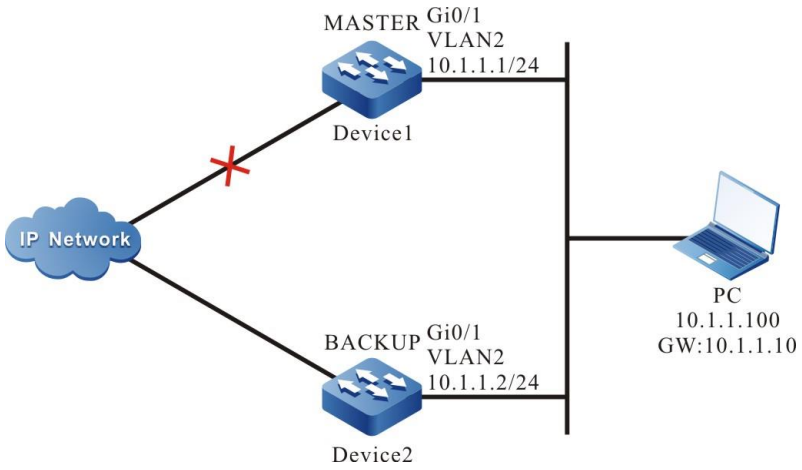


Figure 293 Configure VRRP to link with Track to monitor Master uplink line

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 1336 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*	-
Configure VRRP to associate with the uplink interface	vrrp *vrid* track *interface-name* [*decrement*]	Mandatory By default, the priority consumption value 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 1337 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*	-
Configure VRRP to associate with the uplink interface	vrrp *vrid* track *track-id* [*decrement*]	Mandatory By default, the priority consumption value 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-the Track chapter.
- If the low-pri-master function is configured and when Backup receives the low-priority packet, it 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.

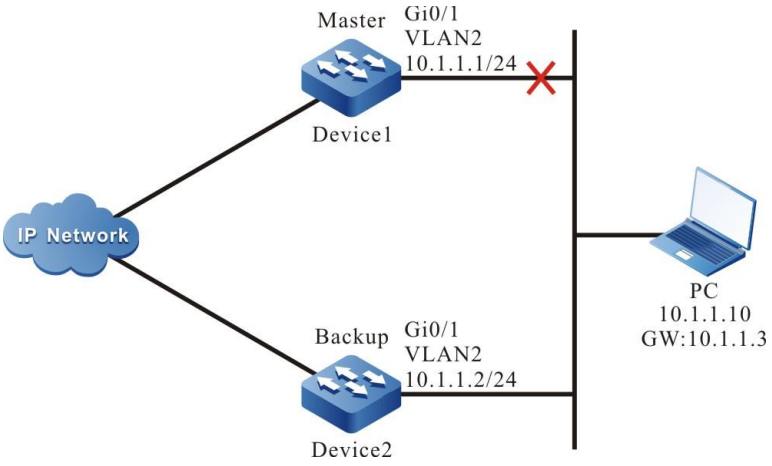


Figure 294 Configure VRRP to associate with track to monitor Master and Backup interconnection line

Table 1338 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*	-
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.

10.5.2.10 VRRP Monitoring and Maintaining

Table 1339 VRRP monitoring and maintaining

Command	Description
show vrrp [interface *interface-name*] | [linkgroup [*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.

10.5.3 VRRP Typical Configuration Example

10.5.3.1 Configure VRRP Single-backup Group

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

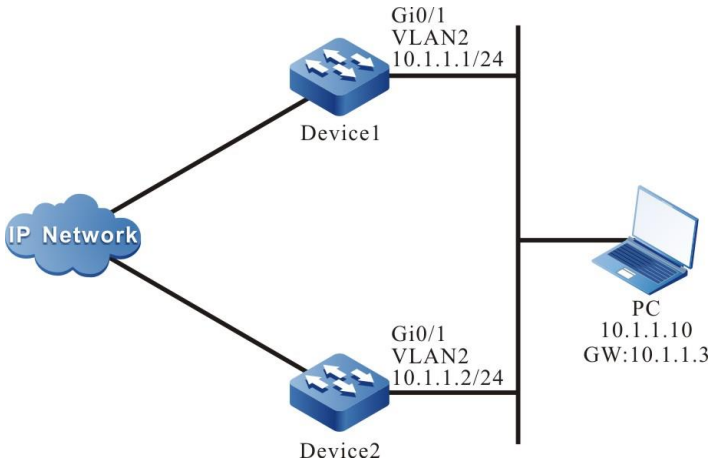


Figure 295 Networking of configuring VRRP single backup group

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 11.1.3, 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 11.1.3.

```
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 s
    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 s
    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.

10.5.3.2 Configure VRRP Multi-Backup Group

Network Requirements

- VRRP multi-backup group is the VRRP link group. On Device1 and Device2 sub interfaces, 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

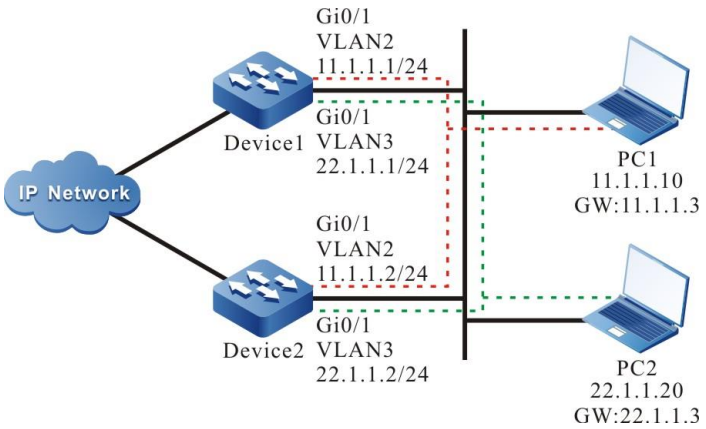


Figure 296 VRRP multi-backup group networking

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 sub 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 sub 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 sub 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 sub 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 s
    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 s
Authentication Mode : None
```

We can see that the VRRP status of the non-Active group and Active group keep consistent.

Step 6: Configure the priority of sub interface 1 in Device1 as 110, making the status change.

```
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#vrrp 1 priority 110
Device1(config-if-gigabitethernet1)#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
  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 s
  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 s
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 s
    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 s
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.

10.5.3.3 Configure VRRP to Link with Track

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

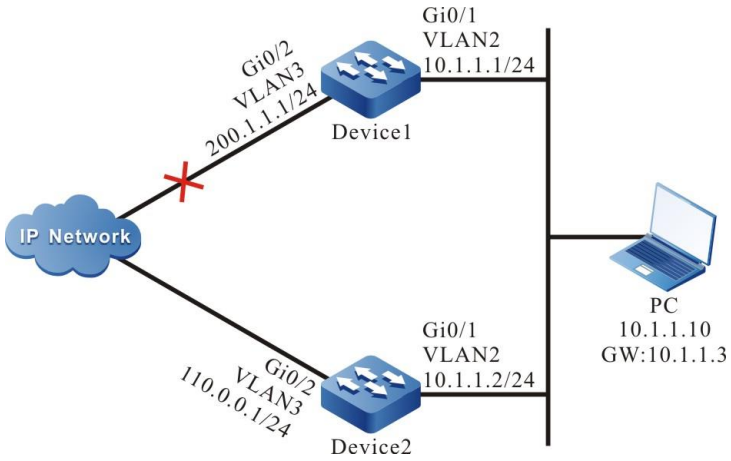


Figure 297 Networking of VRRP linking with Track

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 11.1.3 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 11.1.3.

```
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 s
  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 s
  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 s
  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 s
    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 s
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.

10.5.3.4 Configure VRRP to Link with BFD

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

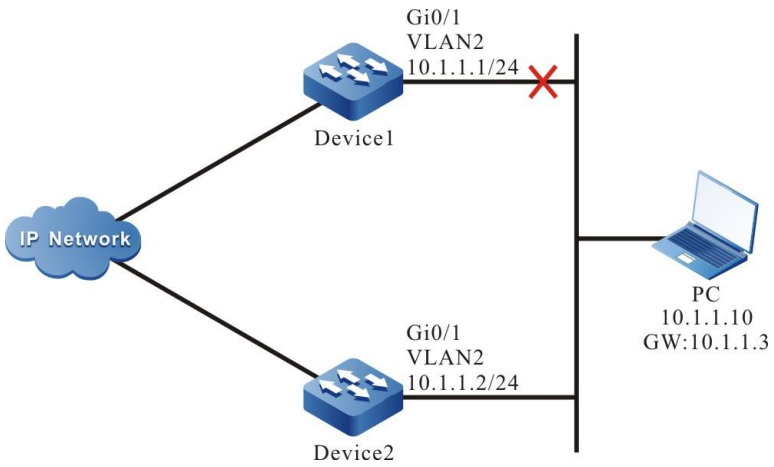


Figure 298 Networking of VRRP linking with BFD

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 11.1.3 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 11.1.3.

```
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 s
    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 s
  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 s
    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 s
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.

10.5.3.5 Configure VRRP Load Balance

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

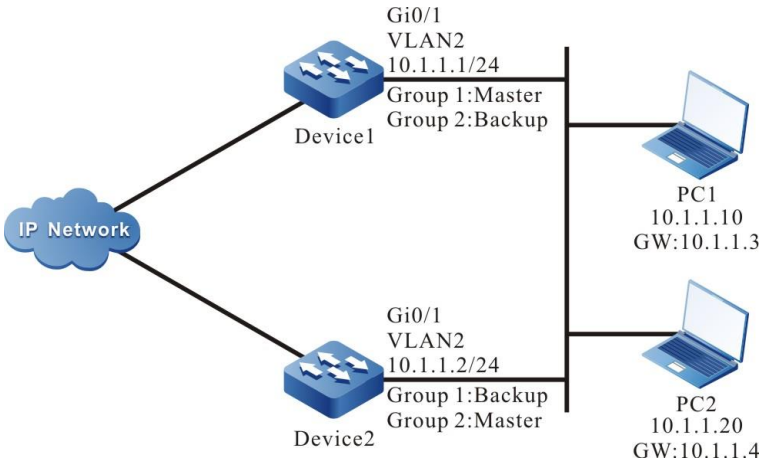


Figure 299 VRRP load balance networking

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 11.1.3 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 11.1.3.

```
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 11.1.4 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 11.1.4 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 s
    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 s
  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 s
    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 s
  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 2. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

10.6 VRRPv3

10.6.1 Overview

VRRPv3 (short for 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”.

10.6.2 VRRPv3 Function Configuration

Table 1340 VRRPv3 function configuration list

Configuration Task	
Configure VRRPv3 basic functions	Enable the VRRPv3 protocol
	Configure the VRRPv3 priority
	Configure the VRRPv3 preemption mode
	Configure the virtual MAC address of VRRPv3
Configure the static VRRPv3 function	Configure the static 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

10.6.2.1 Configure VRRPv3 Basic Functions

In the configuration tasks of VRRPv3, first enable the VRRPv3 protocol and the virtual IPv6 address of the VRRPv3 group needs to be in the same segment as the IPv6 link-local address of the interface so that the configured other functions can take effect.

Configuration Condition

Before configuring the VRRPv3 basic functions, first complete the following task:

- Enable the IPv6 link-local address of the interface

Enable VRRPv3 Protocol

To enable the VRRPv3 function, you need to create the VRRP group and configure the IPv6 link-local virtual address in the interface. To configure the global virtual address, the segment of the virtual address should be in the same segment as the global real address on the interface.

Table 1341 Enable the VRRPv3 protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the link-local virtual address of the VRRPv3 group	ipv6 vrrp *vrid* ip *ip-address* link-local	Mandatory 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 should be in the same segment as the global real address on the interface. By default, do not enable the global virtual address.

Configure 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 1342 Configure the VRRPv3 priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the priority of the VRRPv3 group	ipv6 vrrp *vrid* priority *priority*	Mandatory By default, the priority of VRRPv3 is 100.

Configure 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 1343 Configure the VRRPv3 preemption mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the VRRPv3 group as the preemption mode	ipv6 vrrp *vrid* preempt [delay *delay-time*]	Mandatory By default, enable the preemption function, and the preemption delay time is 0ms.

Note

- When the preemption delay time is the default value, the preemption time is 3 times the message interval plus the delay time.
- When the preemption delay time is not the default value, the preemption time is the preemption delay time plus the delay time.

Configure 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 of the interface.

Table 1344 Configure the real MAC address of VRRPv3

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure VRRPv3 to use the virtual MAC address	ipv6 vrrp *vrid* use-bia	Mandatory By default, VRRPv3 uses the virtual MAC address.

Note

- By default, after configuring VRRPv3, the used is the virtual MAC address. After configuring the command of this section, use the real MAC, that is, when the host sends the packet, forward by the real MAC address; after deleting the command of this section, use the virtual MAC address, that is, when the host sends the packet, use the virtual MAC address to forward.

10.6.2.2 Configure Static VRRPv3 Function

After the static VRRP function is enabled, VRRPv3 does not perform protocol interaction, and the state will eventually remain in the master. The NA response can be performed normally. It is suitable for single device virtual gateway and MLAG scenarios

Configuration Conditions

Before configuring the static VRRPv3 function, first complete the following task:

- Configure one VRRPv3 group

Configure Static VRRP Function

Table 1345 Configure the static VRRPv3

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the static VRRPv3	ipv6 vrrp *vrid* static	Mandatory Configure static VRRPv3. Here, vrid is the VRRPv3 group number.

10.6.2.3 Configure VRRPv3 to Link with Track

VRRPv3 can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRPv3 reliability.

Configuration Condition

Before configuring VRRPv3 to link with Track, first complete the following task:

- Configure one VRRPv3 group

Configure VRRPv3 to Link with Track to Monitor Master Uplink Line

On Master, configure linking with Track. It can link with the interface via Track, or link 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.

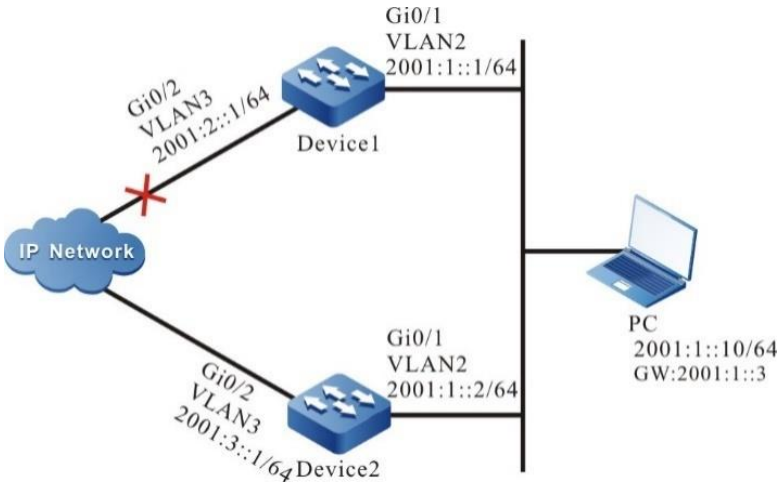


Figure 300 Configure VRRPv3 to link with Track to monitor Master uplink line

Configure VRRPv3 to Link with Track to Link 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 1346 Configure VRRPv3 to link with Track to link 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 VRRPv3 to link with the uplink interface	ipv6 vrrp *vrid* track *interface-name* [*decrement*]	Mandatory By default, VRRPv3 does not link with Track.
Configure the fast switching function when VRRPv3 receives the low-priority packet	ipv6 vrrp *vrid* switchover low-pri-master	Optional By default, do not enable the low-pri-master function. The command is configured on Backup to switch fast when the Master priority is

Step	Command	Description
		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 link 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 1347 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 VRRPv3 to link with the uplink interface	ipv6 vrrp *vrid* track *track-id* [*decrement*]	Mandatory By default, VRRPv3 does not link with Track.
Configure fast switching function when VRRPv3 receives low-priority packet	ipv6 vrrp *vrid* switchover low-pri-master	Optional By default, do not enable the low-pri-master function. 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, it 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 Link with Track to Monitor Master and Backup Interconnection Line

Configure VRRPv3 to link 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.

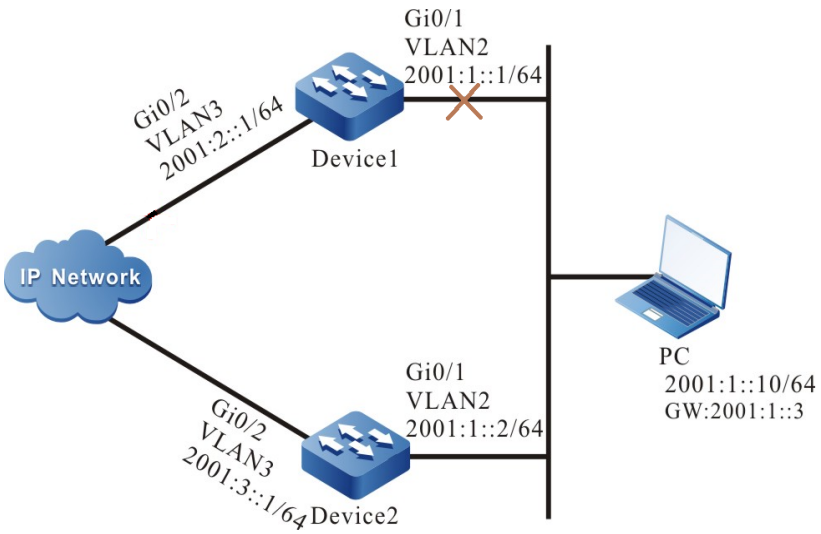


Figure 301 Configure VRRPv3 to link with track to monitor Master and Backup interconnection line

Table 1348 Configure VRRPv3 to link with track to monitor Master and Backup interconnection line

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
Enter the interface configuration mode	interface *interface-name*	Mandatory
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	Mandatory By default, VRRPv3 does not link with Track.

Note

- For the configuration of Track associating BFD and RTR, refer to Track Configuration Manual.
- Track can link with BFD to monitor the status of the line between Master and Backup.

10.6.2.4 VRRPv3 Monitoring and Maintaining

Table 1349 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, link group information and so on.

10.6.3 VRRPv3 Typical Configuration Example

10.6.3.1 Configure IPv6-based VRRP Single-backup Group

Network Requirements

- On Device1 and Device2, create one single IPv6-based 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

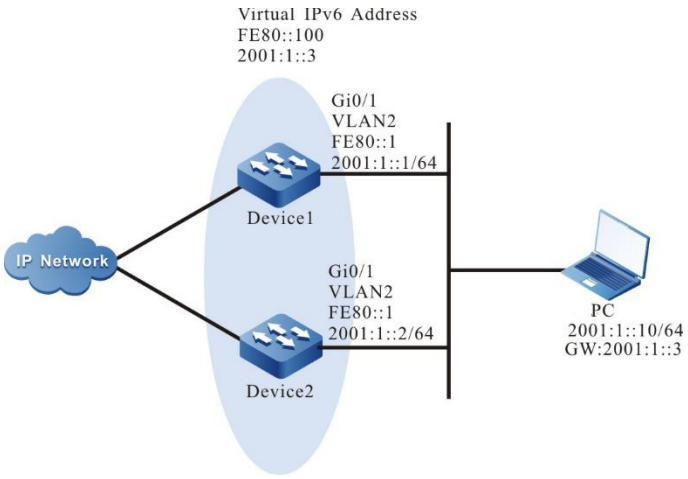


Figure 302 Networking of configuring IPv6-based VRRP single backup group

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface. Enable the switch of the RA response and RA periodical 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-based VRRP group.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 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 VRRPv3 group1 and the virtual IP address is 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 VRRPv3 status of Device1 is Master and the VRRPv3 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 is Master. If the priorities are the same, compare according to the IP link-local address of the interface. The one with large IP address is Master.

10.6.3.2 Configure IPv6-based VRRP to Link with Track

Network Requirements

- On Device1 and Device2, create IPv6 VRRP single backup group; Device1 and Device2 share one virtual IPv6 link-local address and global address,

realizing the backup of the default gateway of the user host, so as to reduce the network interruption time.

- Device1 monitors the status of the interface gigabitethernet1 via Track. When the uplink port gigabitethernet1 of Device1 is down, VRRPv3 can feel the down event of the monitor interface and reduce its own priority, making Backup become the new Master and continue to forward the data.

Network Topology

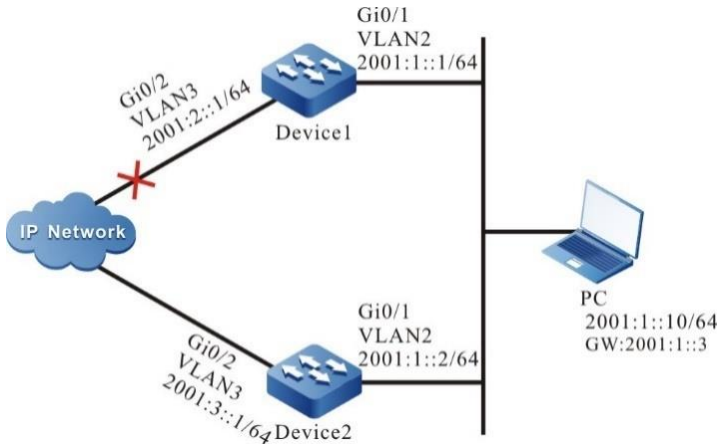


Figure 303 Networking of IPv6 VRRP linking with Track

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface, and enable the switch of the RA response and the RA periodical 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 one IPv6 VRRP group.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 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 VRRPv3 group 1, and the virtual IP address is 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 VRRPv3 to link with Track.

#On Device1, configure VRRPv3 to link with Track, monitor the uplink interface vlan3, and configure the reduced value of the priority 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 monitor interface gigabitethernet1 of Device1 is down, the VRRPv3 priority is reduced by 20. Here, the Device2 priority is high, and preempts as Master, and the status switches.

#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
```

10.6.3.3 Configure IPv6-based VRRP Load Balance

Network Requirements

- On Device1 and Device2, create IPv6 VRRP two backup groups; Device1 and Device2 belong to two VRRPv3 groups at the same time. Device1 is Master in group1 and Backup in group 2; Device2 is Backup in group1 and Master in group 2.
- PC1 forwards data via Device1, and PC2 forwards data via Device2, realizing the load balance.

Network Topology

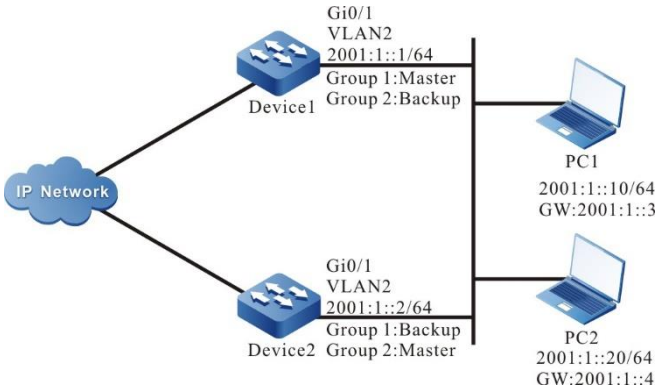


Figure 304 Networking of IPv6 VRRP load balance

Configuration Steps

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

Step 2: Configure the IPv6 address of the interface, and enable the switch of the RA response and RA periodical 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 IPv6 VRRP group 1.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 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 Device1, configure VRRPv3 group 1, and the virtual IP address is 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 IPv6 VRRP group 2.

#On Device1, configure VRRPv3 group2, and the virtual IP address is 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 VRRPv3 group2, the virtual IP address is 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, view the status of the IPv6 VRRP group 1 and group 2.

```
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, view the status of the IPv6 VRRP group 1 and group 2.

```
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

You can see that Device1 serves as Master of VRRPv3 group 1 and becomes Backup of VRRPv3 group 2, while Device2 serves as Master of VRRPv3 group2 and Backup of VRRPv3 group 1. When one device fails, two PCs forward data via the other device. This not only takes effect of load balance, but also realizes the mutual backup.

10.7 VBRP

10.7.1 Overview

VBRP (Virtual Backup Router Protocol) provides one backup function for the gateway, used by multiple devices to maintain the continuous forwarding of the virtual gateway. VBRP maps the referred multiple devices to one virtual router and ensures that there is only one device to represent for the virtual router to forward packets. When the device for forwarding data cannot work normally because of some reason, another standby device replaces the virtual router to forward packets, while the device that cannot work normally does not bear the forwarding task any more. The switching process is short and it is transparent for the host in the LAN, so as to reach the backup function for the gateway.

The active device mentioned in the following text is replaced by “Active” and the standby device is replaced by “Standby”.

10.7.2 VBRP Function Configuration

Table 1350 VBRP function configuration list

Configuration Task	
Configure the VBRP basic functions	Enable the VBRP protocol

Configuration Task	
	Enable the VBRP priority
	Enable the VBRP preemption mode
	Configure the VBRP real MAC address
Configure the VBRP network authentication	Configure the VBRP simple text authentication
	Configure the VBRP MD5 authentication
Configure VBRP to link with Track to associate with the uplink interface	Configure VBRP to link with Track to associate with the uplink interface
	Configure VBRP to link with Track to associate with the MLAG role

10.7.2.1 Configure VBRP Basic Functions

In the configuration tasks of VBRP, first enable the VBRP function and the virtual IP address of the VBRP group needs to be in the same segment as the interface IP address so that the configured other functions can take effect.

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the interface IP address

Enable VBRP Protocol

To enable the VBRP function, we need to create the VBRP group in the interface and add the VBRP device to the group.

Table 1351 Enable the VBRP protocol

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

Step	Command	Description
Configure the VBRP group	standby [*group-number*] ip [*ip-address*]	Mandatory Configure the device to add to the VBRP group. The default value of *group-number* is 0. *ip-address* is the virtual IP address.

Configure VBRP Priority

After configuring VBRP and if not setting the priority, the default priority is 100. The device with high priority is elected as Active for forwarding the packet and the other become Standby. 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 Active. We can set the VBRP priority as desired. The larger the value, the higher the priority.

Table 1352 Configure the VBRP priority

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the priority of the VBRP group	standby [*group-number*] priority *value*	Mandatory Configure the VBRP priority. By default, the VBRP priority is 100.

Configure VBRP Preemption Mode

In the preemption mode, once other device in the VBRP group discovers that its priority is higher than that of the current Active, it becomes Active; in non-preemption mode, as long as Active does not fail, even the other device has higher priority, it cannot become Active.

Table 1353 Configure the VBRP preemption mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the VBRP group as the preemption mode	standby [*group-number*] preempt [delay *delay-time*]	Mandatory Configure the VBRP preemption mode. By default, it is the non-preemption mode.

Configure VBRP Real MAC Address

After configuring VBRP and if it is necessary to make the VBRP group use the real MAC address, we need to use the following command to configure. When the virtual router replies the ARP request, the replied is real MAC address, but not the virtual MAC address of the interface. By default, the used is the virtual MAC address.

Table 1354 Configure the VBRP real MAC

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure VBRP as the virtual MAC	standby [*group-number*] use-bia	Mandatory By default, use the virtual MAC address.

Note

- By default, after configuring VBRP, the used is the virtual MAC address. After configuring the command **standby use-vmac**, use the real MAC, that is, when the host sends the packet, forward by the real MAC address; after configuring the command **no standby use-vmac**, use the virtual MAC

address of the interface, that is, when the host sends the packet, use the virtual MAC address to forward.

10.7.2.2 Configure VBRP Network Authentication

VBRP has two modes, that is, simple text authentication and MD5 authentication. The set length of the simple text authentication cannot exceed eight authentication words. The set length of the MD5 authentication is the authentication word not exceeding 64 bits.

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the VBRP group

Configure VBRP Simple Text Authentication

Configure the VBRP authentication to check and verify the validity of the VBRP packet. We can use the following command to configure the VBRP simple text authentication mode.

Table 1355 Configure the VBRP simple text authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the VBRP simple text authentication	standby *group-number* authentication { *string* }	Mandatory The configured authentication word is string and the length cannot exceed 8-bit authentication word. By default, do not enable the simple text authentication.

Configure VBRP MD5 Authentication

Configure the VBRP authentication to check and verify the validity of the VBRP packet. We can use the following command to configure the VBRP MD5 authentication mode.

Table 1356 Configure the VBRP MD5 authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the VBRP MD5 authentication	standby *group-number* authentication { md5 { key-id *key-identifier* key-string *key-string* } | { key-string *key-string* } }	Mandatory Configure the MD5 network authentication and the length cannot exceed 8-bit authentication word. By default, do not enable the MD5 authentication.

10.7.2.3 Configure VBRP to Associate with Uplink Port via Track

Associate VBRP with the concerned uplink interface via Track. When the uplink interface is down, Active automatically reduces its own priority. Here, Standby receives the low-priority packet and switches to Active. For details, refer to the following figure.

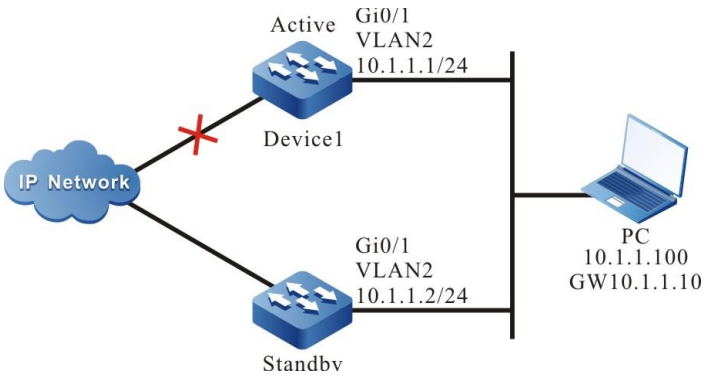


Figure 305 Configure VBRP to link with Track to monitor Active uplink line

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the VBRP group

Configure VBRP to Link with Track to Associate with Uplink Interface

Associate VBRP with the concerned uplink interface via Track. When the uplink interface is down, Active automatically reduces its own priority. Here, Standby receives the low-priority packet and switches to Active.

Table 1357 Configure VBRP to link with Track to associate with the uplink interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure VBRP to link with Track to associate with the uplink interface	standby [*group-number*] track { { *interface-name*} | *track-id* } [*decrement*]	Mandatory Configure associating with the *interface-name* interface. When the interface is down, the priority reduces by decrement. By default, reduce the priority to 10.

Configure VBRP to Link with Track to Associate with BFD and RTR

If Track is associated with BFD, RTR and so on, Active can directly associate with the Track group, so as to monitor the line. When the line fails, Active reduces its own priority. Here, Standby receives the low-priority VBRP packet, switch to Active.

Table 1358 Configure VBRP to link with Track to associate with BFD and RTR

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure VBRP to link with Track to associate with the	standby [*group-number*] track { *track-id* } [*decrement*]	Mandatory Configure associating with

Step	Command	Description
uplink interface		Track *track-id.* The Track is associated with BFD, RTR and so on. By default, the priority is reduced by 10.

Note

- For the configuration method of associating Track with BFD, RTR and so on, refer to Track Configuration Manual.

Configure VBRP to Link with Track to Associate with MLAG Role

After configuration, the MLAG master device can perform protocol interaction, and the MLAG slave device does not perform protocol interaction, and the state is standby.

Table 1359 Configure VBRP to link with Track to associate with MALG role

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure VBRP to link with Track to associate with MALG role	standby [*group-number*] track mlag role	Mandatory Configure the associated MLAG role. Here, group-number is the VBRP group number.

10.7.2.4 VBRP Monitoring and Maintaining

Table 1360 VBRP monitoring and maintaining

Command	Description
show standby [brief] | [all] | [interface *interface-name* group gid]	Display the VBRP 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.

10.7.3 VBRP Typical Configuration Example

10.7.3.1 Configure VBRP Basic Mode

Network Requirements

- Enable VBRP between Device1 and Device2; Device1 and Device2 share one virtual IP address, realizing the backup for the default gateway of the user host and reducing the network interruption time.

Network Topology

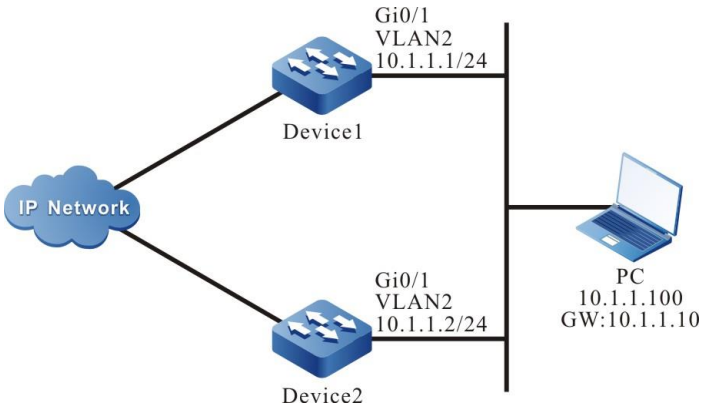


Figure 306 Networking of VBRP basic mode

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 VBRP group.

#Configure VBRP group 1 on Device1; the virtual IP address is 11.1.1.10; enable the preemption mode; configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#Configure VBRP group 1 on Device2; the virtual IP address is 11.1.1.10; enable the preemption mode;

```
Device2#configure terminal
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

Step 4: Check the result.

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 193.168.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.633348 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2,priority 100 (expires in 8.466648 secs)
  Priority 110 (configured 110)
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
```

```
Local virtual MAC address is 0000.0c07.ac01
Current MAC type VMAC
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.450022 secs
Preemption enabled, delay 0 sec
Active router is 10.1.1.1, priority 110 (expires in 7.266656 secs)
Standby router is local
Priority 100 (configured 100)
```

From the VBRP status, we can see that the VBRP priority of Device1 is 110, the status is Active, and the VBRP status of Device2 is Standby. After Device1 fails, Device2 automatically switches to Active for forwarding data.

Note

- The election principle of the VRRP status is by priority. The one with large priority is Active. If the priorities are the same, compare according to the IP address of the interface. The one with large IP address is Active.
- By default, VBRP works in the non-preemption mode. The preemption mode needs to be configured manually. It is recommended to configure as the preemption mode.
- The default priority of VBRP is 100.

10.7.3.2 Configure VBRP to Link with Track

Network Requirements

- Enable VBRP between Device1 and Device2.
- Device1 monitors the interface VLAN3 status via Track. When the uplink port VLAN3 of Device1 is down, VBRP can feel and switch the status, making Standby become new Active for forwarding data.

Network Topology

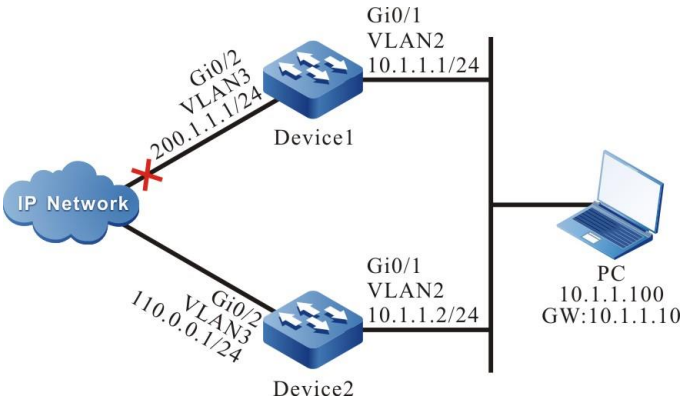


Figure 307 Networking of configuring VBRP to link with Track

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 VBRP group.

#Configure the virtual IP address of VBRP group 1 on Device1 as 11.1.10, enable the preemption function, and configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#Configure the virtual IP address of VBRP group1 on Device2 as 11.1.10 and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 1 ip 10.1.1.10
Device2(config-if-vlan2)#standby 1 preempt
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
```

```
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.533352 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 9.283362 secs)
  Priority 110 (configured 110)
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.516646 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.1, priority 110 (expires in 9.516646 secs)
  Standby router is local
  Priority 100 (configured 100)
```

Step 4: Configure VBRP to link with Track.

#On Device1, configure VBRP to link with Track, monitor the uplink interface vlan3, and configure the priority decrement as 20.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 track vlan 3 20
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
```

```
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.533352 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 9.283362 secs)
  Priority 110 (configured 110)
 Track interface vlan3 state Up decrement 20
```

#When the uplink port of Device1 VLAN3 is down, its VBRP priority is reduced by 20. At this time, the priority of Device2 is high, so state switching will occur.

#View the VBRP status of Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.800008 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.2, priority 100 (expires in 7.766676 secs)
  Standby router is local
  Priority 90 (configured 110)
    Track interface vlan3 state Down decrement 20
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.533352 secs
```

Preemption enabled, delay 0 sec
Active router is local
Standby router is 10.1.1.1, priority 90 (expires in 9.283362 secs)
Priority 100 (configured 100)

10.7.3.3 Configure VBRP Load Balance Mode

Network Requirements

- Device1 and Device2 belong to two VBRP groups at the same time; Device1 is Active in group1 and Standby in group2; Device2 is Standby in group1 and Active in group2.
- PC1 forwards data via Device1 and PC2 forwards data via Device2, realizing the load balance.

Network Topology

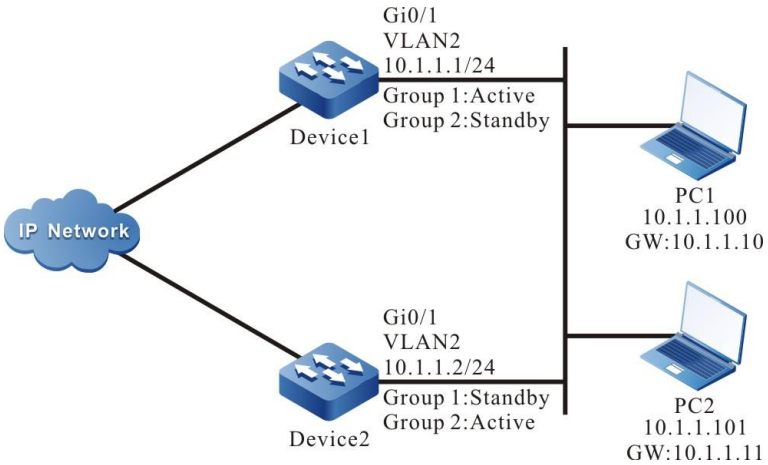


Figure -308 Networking of VBRP load balance

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 VBRP group1.

#Configure the virtual IP address of VBRP group 1 on Device1 as 11.1.10, enable the preemption function, and configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 1 ip 10.1.1.10
Device1(config-if-vlan2)#standby 1 preempt
Device1(config-if-vlan2)#standby 1 priority 110
```

#Configure the virtual IP address of VBRP group1 on Device2 as 11.1.10 and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 1 ip 10.1.1.10
Device2(config-if-vlan2)#standby 1 preempt
```

Step 4: Create VBRP group2.

#Configure the virtual IP address of VBRP group 2 on Device1 as 11.1.11, and enable the preemption function.

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#standby 2 ip 10.1.1.11
Device1(config-if-vlan2)#standby 2 preempt
```

#Configure the virtual IP address of VBRP group 1 on Device2 as 11.1.11, enable the preemption function, and configure the priority as 120.

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#standby 2 ip 10.1.1.11
Device2(config-if-vlan2)#standby 2 preempt
Device2(config-if-vlan2)#standby 2 priority 120
```

Step 5: Check the result.

#View the status of VBRP in group 1 and group 2 on Device1.

```
Device1#show standby
Interface vlan2
  Primary address 10.1.1.1, state up
Group 1
  State is Active
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.1/24
```

```
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.633348 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 10.1.1.2, priority 100 (expires in 7.83370 secs)
  Priority 110 (configured 110)
Group 2
  State is Standby
  Virtual IP address is 10.1.1.11
  Refer to local IP prefix 10.1.1.1/24
  Local virtual MAC address is 0000.0c07.ac02
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.950002 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.2, priority 120 (expires in 7.300028 secs)
  Standby router is local
Priority 100 (configured 100)
```

#View the status of VBRP in group 1 and group 2 on Device2.

```
Device2#show standby
Interface vlan2
  Primary address 10.1.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 10.1.1.10
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type VMAC
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.600016 secs
  Preemption enabled, delay 0 sec
  Active router is 10.1.1.1, priority 110 (expires in 7.700012 secs)
  Standby router is local
  Priority 100 (configured 100)
Group 2
  State is Active
  Virtual IP address is 10.1.1.11
  Refer to local IP prefix 10.1.1.2/24
  Local virtual MAC address is 0000.0c07.ac02
  Current MAC type VMAC, installed into HW
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.816674 secs
```

```
Preemption enabled, delay 0 sec
Active router is local
Standby router is 10.1.1.1, priority 100 (expires in 8.33332 secs)
Priority 120 (configured 120)
```

We can see that Device1 serves as Active of VBRP group1 and Standby of VBRP group2. In contrast with Device1, Device2 serves as Active of VBRP group 2 and Standby of VBRP group 1. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

10.8 VRRP Load-Balance Protocol

10.8.1 Overview

VRRP load-balance protocol (Load-Balance Virtual Router Redundancy Protocol) supports the clients configured with the same gateway to be loaded dynamically under the condition of multiple gateway exports in LAN. Meanwhile, it takes into account the redundancy backup feature.

The main devices mentioned below are replaced by "Master" and the backup devices are replaced by "Backup".

10.8.2 VRRP Load-balance Protocol Function Configuration

Table 1361 VRRP load-balance protocol function configuration list

Configuration tasks	
Configure the VRRP current mode	Enable the VRRP load balance mode
Configure the basic functions of the VRRP load balance protocol	Enable the VRRP load balance protocol
	Configure the priority of the VRRP load balance protocol
	Configure the virtual MAC address of the VRRP load balance protocol
Configure the timer of the VRRP load balance protocol	Configure the period interval of the Hello packet
	Configure the period interval of the Keep packet
	Configure the zombie timer of the virtual mac address

Configuration tasks	
	Configure the age timer of the forwarding terminal
	Configure the detection timer of the forwarding terminal

10.8.2.1 Configure the Current Mode of the VRRP Load-balance Protocol

In the configuration tasks of VRRP load balancing protocol, the VRRP load balancing protocol mode must be enabled, which is mutually exclusive with the VRRP standard protocol.

Configuration Conditions

None

Enable VRRP Load-Balance Protocol Mode

Table 1362 Enable the VRRP load-balance protocol mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Global configuration mode	vrrp mode load-balance	Mandatory

10.8.2.2 Configure the Basic Functions of VRRP Load-Balance Protocol

In the configuration tasks of the VRRP load-balance protocol, the VRRP load-balance protocol must be enabled first, and the virtual IP address of the VRRP load-balance protocol group needs to be in the same network segment as the IP address of the interface, so the other configured functions can take effect.

Configuration Conditions

Before configuring the VRRP basic functions, first complete the following tasks:

- Configure the IP address of the interface

Enable the VRRP Load-Balance Protocol

To enable the VRRP load-balance protocol function, it is necessary to create one VRRP load-balance protocol group in the interface and configure the virtual IP address.

Table 1363 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 load-balance protocol group	vrrp *vrid* ip *ip-address*	Mandatory Enable the VRRP load-balance protocol. Here, vrid is the VRRP load-balance protocol group number, and ip-address is the virtual IP address.

Note

- In the VRRP load-balance protocol mode, you cannot configure the virtual IP to be the same as the interface IP.

Configure the VRRP Load Balancing Protocol Priority

If the priority is not configured after configuring VRRP load balancing protocol, its default priority is 100; the device with high priority will be elected as Master responsible for forwarding packets, and the others will be Backup; if the priorities of all devices are equal, elect according to the interface IP address of each device, and the interface with the large IP address will be Master; you can set the priority of the VRRP load-balance protocol according to the need. The larger the priority value is, the higher the priority is.

Table 1364 Configure the priority of the VRRP load-balance protocol group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the priority of the VRRP load-balance protocol group	vrrp *vrid* priority *priority*	Mandatory By default, the priority is 100.

Configure Simple Text Authentication of VRRP Load Balancing Protocol

After configuring VRRP load balancing protocol, if simple text authentication is not set, the simple text authentication function is not enabled by default; Only when the authentication in VRRP load balancing protocol group is consistent can the neighbor be established successfully and the negotiation status be carried out.

Table 1365 Configure simple text authentication of VRRP load balancing protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure simple text authentication of VRRP load balancing protocol	vrrp *vrid* authentication text *string*	Mandatory By default, do not enable simple text authentication function. The authentication password is eight characters at most.

Configure the Real MAC Address of the VRRP Load-balance Protocol

Each virtual router in a VRRP load balancing protocol group has a virtual MAC address. According to the regulations of the VRRP load balancing protocol, the format of the virtual MAC address is 00.01.7a.00. {vrid}. {mid}, and the mid value is assigned by the master. When a virtual router responds to an ARP request, the returned is the

virtual MAC address, not the real MAC address of the interface. By default, the virtual MAC address of the interface is used.

Table 1366 Configure the real MAC address of the VRRP load-balance protocol

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the VRRP load-balance protocol to use the real MAC address	vrrp *vrid* use-bia	Mandatory By default, use the virtual MAC address.

Note

- By default, adopt the virtual MAC address on the corresponding interface after configuring VRRP. After configuring the command of this section, use the real MAC, that is, the host forwards the packet by the real MAC address; after deleting the command of this section, use the virtual MAC address of the corresponding interface, that is, the host sends the packet by the virtual MAC address.

10.8.2.3 Configure the Timer of the VRRP Load-Balance Protocol

In the VRRP load-balance protocol, perform the corresponding actions according to the corresponding timer, so as to maintain the relevant state.

Configuration Conditions

Before configuring the timer of the VRRP load-balance protocol, first complete the following tasks:

- Switch the VRRP mode to the VRRP load-balance protocol mode

- Enable the VRRP load-balance protocol group

Configure the Period Interval of the Hello Packet

The Hello packet is mainly responsible for announcing some information to the neighbors and maintaining the relationship between neighbors, so it is necessary to keep the sending periods of the Hello packets consistent among neighbors in the same group.

Table 1367 Configure the period interval of the Hello packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the period interval of the Hello packet of the VRRP load-balance protocol group	vrrp *vrid* timers hello *Hello–time* [hold *Hold–time* [preserved *Preserved–time* [delay-vote *Delay-vote–time*]]]	Mandatory Configure the period interval of the Hello packet. Here, vrid is the VRRP group number; Hello–time specifies the sending period of the Hello packet of the VRRP group; Hold–time specifies the hold time of the VRRP group neighbor; Preserved–time specifies the reserve time of the virtual MAC of the VRRP group; Delay-vote–time specifies the delay election time of the VRRP group.

Configure the Period Interval of the Keep Packet

The Keep packet is responsible for advertising the virtual MAC address of the virtual router to the L2 switch, and refreshing the L2 MAC entries of the switch.

Table 1368 Configure the period interval of the Keep packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the period interval of the Keep packet of the VRRP load-balance protocol group	vrrp *vrid* timers keep *keep-time*	Mandatory Configure the period interval of the Keep packet. Here, vrid is the VRRP group number; Keep-time specifies the period of sending the Keep packet of the VRRP load-balance protocol group.

Configure the Zombie Timer of the Virtual MAC Address

After the owner of the virtual MAC fails, the virtual MAC will experience the reserved state, and reach the zombie state. The configuration of the zombie state needs the timer larger than the age time of the bottom terminal ARP.

Table 1369 Configure the zombie timer of the virtual MAC address

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the zombie time of the virtual MAC address of the VRRP load-balance protocol group	vrrp *vrid* timers zombie *zombie-time*	Mandatory Configure the zombie timer of the virtual MAC address. Here, vrid is the VRRP load-balance protocol group number, and Zombie-time specifies the zombie time of the virtual MAC of

Step	Command	Description
		the VRRP load-balance protocol group.

Configure the Age Timer of the Forwarding Terminal

If the terminal is not online for a long time when managing the terminal at the forwarding layer, it will be aged to release the resources occupied by the terminal, thereby refreshing the terminal table items of the group.

Table 1370 Configure the age timer of the terminal at the forwarding layer

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the age timer of the forwarding terminal of the VRRP load-balance protocol group	vrrp *vrid* timers forwarding ageing *forwarding-ageing-time*	Mandatory Configure the age time of the terminal at the forwarding layer. Here, vrid is the VRRP group number, and forwarding-ageing-time specifies the age time of the terminal at the forwarding layer in the VRRP group.

Configure the Detection Timer of the Terminal at the Forwarding Layer

When managing the terminal at the forwarding layer, detect the online state of the terminal regularly, so as to update the state of the terminal at the local.

Table 1371 Configure the detection timer of the terminal at the forwarding layer

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	Mandatory
Configure the detection timer of the terminal at the forwarding layer in the VRRP load-balance protocol group	vrrp *vrid* timers forwarding dtct *forwarding-dtct-time*	Mandatory Configure the detection timer of the terminal at the forwarding layer. Here, vrid is the VRRP load-balance protocol group number, and forwarding-dtct-time specifies the detection time of the terminal at the forwarding layer in the VRRP load-balance protocol group.

10.8.2.4 Monitoring and Maintaining of VRRP Load-balance Protocol

Table 1372 VRRP monitoring and maintaining

Command	Description
Show vrrp [interface interface-name]	Display the VRRP load-balance protocol configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, linkage group information, etc.

10.8.3 VRRP Load-balance Typical Configuration Example

10.8.3.1 Configure the Basic Functions of the VRRP Load-balance Protocol

Network Requirements

- On Device1 and Device2, create one VRRP load-balance backup group, making Device1 and Device2 share one virtual IP address and realizing the backup for the default gateway of the user host, so as to reduce the interruption time of the network.
- The VRRP load-balance protocol realizes the load function by distributing the traffic from different user hosts to different VRRP devices in a group. The significant difference from the common VRRP is that backup devices in the VRRP load-balance protocol can also forward the traffic, which enables users to configure the same gateway address for all hosts in the network to achieve load balancing.

Network Topology

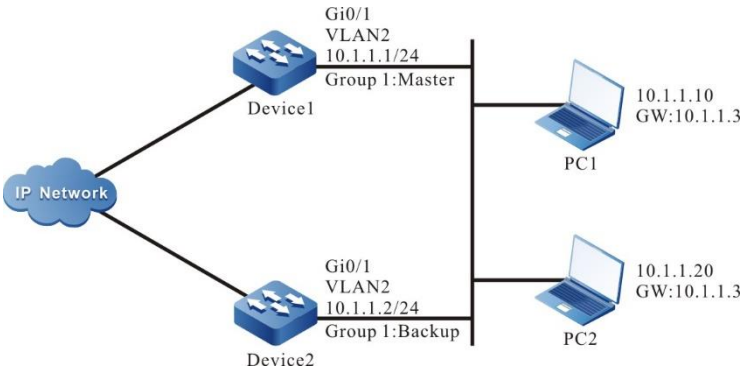


Figure 309 Networking of configuring the basic functions of the VRRP load-balance protocol

Configuration Steps

Step 1: Configure the IPv4 address of the interface (omitted).

Step 2: Configure the device as the VRRP load-balance protocol mode.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#vrrp mode load-balance
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#vrrp mode load-balance
```

#Query the VRRP protocol mode of Device1.

```
Device1#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

#Query the VRRP protocol mode of Device2.

```
Device2#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

You can see that both Device1 and Device2 run in the VRRP load-balance protocol mode.

Step 3: Create one VRRP load-balance protocol backup group.

#On Device1, create backup group 1. The virtual IP address is 11.1.3, and configure the priority as 110.

```
Device1(config)#interface vlan2
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, create backup group 1, and the virtual IP address is 11.1.3

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if- vlan2)#exit
```

Step 4: Query the status of the VRRP load-balance protocol.

#Query the VRRP load-balance protocol neighbor table of Device1.

```
Device1#show vrrp neighbor

 Gid  Neighbor  Priority  Uid     Virtual-ip  Master    Hold-time  Interface
 1    10.1.1.2  100       412780  10.1.1.3    10.1.1.1  36         vlan2
```

From the Neighbor field, you can see that Device1 successfully sets up the neighbor with Device2.

#Query the VRRP load-balance protocol neighbor table of Device2.

```
Device2#show vrrp neighbor

 Gid  Neighbor  Priority  Uid     Virtual-ip  Master    Hold-time  Interface
 1    10.1.1.1  110       348619  10.1.1.3    10.1.1.1  33         vlan2
```

From the Neighbor field, you can see that Device2 also sets up the neighbor with Device1 successfully.

#Query the VRRP load-balance protocol status of Device1.

```
Device1#show vrrp
Interface vlan2
  Vrf:0
  Virtual router : 1
    Mac mode: virtual mac mode
    Forwording mac :
      00.01.7a.00.01.01 ,installed into HW
    Virtual IP address : 10.1.1.3
    Match address : 10.1.1.1
    State : Master
    Priority : 110
    Hello interval(sec) :  10
      next hello in 3 secs
    Hold time(sec) :       40
    Delay vote time(sec) : 40
    Delay delete time(sec) : 20
    Preserve time(sec) :   40
    Keep(min) : 15
    Zombie(min) : 10
    Uid : 348619
    Terminal number : 0/1000
```

From the State field, you can see that Device1 is elected as Master.

#Query the VRRP load-balance protocol status of Device2.

```
Device2#show vrrp
Interface vlan2
  Vrf:0
  Virtual router : 1
    Mac mode: real mac mode
    Forwording mac :
      00.01.7a.00.01.02 ,installed into HW
    Virtual IP address : 10.1.1.3
    Match address : 10.1.1.2
    State : Backup
    master:10.1.1.1
    Priority : 100
    Hello interval(sec) :  10
      next hello in 6 secs
    Hold time(sec) :       40
    Delay vote time(sec) : 40
    Delay delete time(sec) : 20
    Preserve time(sec) :   40
    Keep(min) : 15
    Zombie(min) : 10
    Uid : 412780
    Terminal number : 0
```

From the State field, you can see that Device2 becomes Backup.

#On Device1, query the VRRP load-balance protocol forwarding the MAC address distributing table.

```
Device1# show vrrp fmac

 Gid Virtual-ip Forwarding-mac   Owner     Backup   Owner-state Timeout  Interface
1   10.1.1.3   0101.7a00.0101   10.1.1.1  -       Active       -       vlan2
1   10.1.1.3   0101.7a00.0102   10.1.1.2  -       Active       -       vlan2
```

Only Master has the function of distributing the forwarding MAC address. From the corresponding relationship between Owner and Forwarding-mac, it can be seen that the forwarding MAC address allocated for 11.1.1 is 0101.7a7c.7226, and the forwarding MAC address allocated for 11.1.2 is 0101.7aff.ff00.

Note

- VRRP load balancing protocol can only work in non-preempt mode.
- VRRP load balancing protocol starts the delay election timer in the init state, and by default, it is four times of the Hello interval. Elect after timeout.
- VRRP load balancing protocol elects according to the priority. The one with the highest priority is elected as Master If the priorities are the same, compare the IP addresses of the interfaces. The one with largest IP address is elected as Master, and the others are Backup.

Step 5: Check the result.

#On PC1 and PC2, ping the gateway to test the connectivity. On Device1, query the gateway forwarding MAC address distributed by Master for the host.

```
Device1#show vrrp terminal

 Gid    Virtual-ip      Terminal         Forwarding-mac    Interface
 1      10.1.1.3        10.1.1.10        0101.7a00.0101    vlan2
 1      10.1.1.3        10.1.1.20        0101.7a00.0102    vlan2
```

As shown in the table above, the host terminals PC1 and PC2 are assigned with different gateway forwarding MAC addresses. Combined with the forwarding MAC addresses allocated by Master for Device 1 and Device 2 in Step 4, it can be seen that the traffic of PC1 and PC2 is forwarded by Device 1 and Device 2 respectively to achieve load balancing.

#On Device2, query the forwarding MAC address distributing table of the Backup terminal gateway.

```
Device2#show vrrp terminal

 Gid    Virtual-ip      Terminal         Forwarding-mac    Interface
 1      10.1.1.3        10.1.1.10        0101.7a00.0101    vlan2
 1      10.1.1.3        10.1.1.20        0101.7a00.0102    vlan2
```

Master synchronizes the forwarding MAC address distributing table of the terminal gateway to all VRRP devices.

10.9 Track

10.9.1 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.

10.9.2 Track Function Configuration

Table 1373 Track function configuration list

Configuration Task	
Configure the Track group	Configure the Track group
Configure the monitor object	Configure monitoring the interface status
	Configure monitoring the direct route of the interface
	Configure monitoring the bandwidth utilization alarm at the ingress and egress directions of the interface
	Configure monitoring route reachable
	Configure monitoring the aggregation group status
	Configure monitoring L2 Ethernet interface status
	Configure monitoring the RTR group
	Configure monitoring the BSM instance
	Configure monitoring the BFD session

10.9.2.1 Configure Track Group

Configuration Condition

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 1374 Configure the Track group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the Track group	track *track-id*	Mandatory
Configure Track group logic	logic { operator [AND | OR] | reverse }	Optional AND: logic “and” OR: logic “or” reverse: logic reverse By default, Track group logic is “and”; the logic reverse function does not take effect.

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.

10.9.2.2 Configure Monitor Object

Configuration Condition

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 1375 Configure monitoring interface IPv4 status

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track-id*	-
Configure monitoring interface status	interface *interface-name* line-protocol	Mandatory

Table 1376 Configure monitoring the IPv6 status of the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *track-id*	-
Configure monitoring the interface status	**interface** *interface-name* **line-ipv6-protocol**	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 1377 Configure monitoring the direct route of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track-id*	-
Configure monitoring the direct route of the interface	interface *interface-name* ip-routing	Mandatory

Table 1378 Configure monitoring the IPv6 direct route of the interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track-id*	-
Configure monitoring the direct route of the interface	interface *interface-name* ipv6-routing	Mandatory

Configure Monitoring Interface Bandwidth Utilization Alarm

In the track group, the monitoring object can be configured as the bandwidth utilization alarm in the input or output direction of the interface. When the inbound traffic of the interface is higher than the inbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is up; When the inbound traffic of the interface is lower than the inbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is down; When the outbound traffic of the interface is higher than the outbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is up; When the outbound traffic of the interface is lower than the outbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is down.

Table 1379 Configure monitoring interface bandwidth utilization alarm

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-

Step	Command	Description
Configure the direct route of the monitoring interface	interface *interface-name* trap-threshold [input | output]	Mandatory

Note

- For the configuration of the alarm value of the interface bandwidth, refer to the interface configuration manual.

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 1380 Configure monitoring IPv4 route reachable

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring route reachable	ip-route { *ip-address network mask* | *mask-len* } [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.

Table 1381 Configure monitoring IPv6 route reachable

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring route reachable	ipv6-route *ipv6-address/mask-length* [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 Aggregation Group Status

You can configure the monitoring object in the track group is the status of the aggregation group. When the aggregation group status is up, the monitoring object status is up; When the aggregation group status is down, the monitoring object status is down.

Table 1382 Configure monitoring aggregation group status

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	Mandatory
Configure monitoring aggregation group status	link-aggregation *link-aggregation-id*	Mandatory

Configure Monitoring L2 Ethernet Interface Status

You can configure the monitoring object in the track group is the state of L2 Ethernet interface. When the L2 Ethernet interface is up, the monitoring object status is up; When the L2 Ethernet interface is down, the status of the monitoring object is down.

Table 1383 Configure monitoring L2 Ethernet interface status

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track track -id	Mandatory
Configure monitoring L2 Ethernet interface status	switchport interface-name	Mandatory

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 1384 Configure monitoring the RTR group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
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 BSM Entity

You can configure the monitoring object in the Track group as BSM (business sensitivity measure) entities. When the connectivity of BSM entity is reachable, the status of monitoring object is up; When the connectivity of the BSM entity is unreachable, the state of the monitoring object is down. BSM detects and monitors network communication by sending specified protocol packets regularly. Track can indirectly monitor the network communication by monitoring the connectivity of BSM

entities.

Table 1385 Configure monitoring the BSM entity

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring BSM entity	bsm *bsm-entity-id* probe	Mandatory

Note

- For the related configuration of BSM entity, refer to the BSM 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 1386 Configure monitoring the BFD IPv4 single-hop session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
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,

Step	Command	Description
		the BFD session cannot be set up successfully.

Table 1387 Configure monitoring the BFD IPv6 single-hop session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring the BFD session	bfd interface *interface-name* remote-ipv6 *ipv6-address* local-ipv6 *ipv6-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 1388 Configure monitoring the BFD IPv4 multiple-hop session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring the BFD session	bfd multihop control remote-ip *ip-address* local-ip *ip-address* { [vrf *vrf-name*] | [interface *interface-name*] } [multiplier *multiplier-value* min-transmit-interval *minimum-transmit-interval-value* min-receive-interval *minimum-receive-interval-value*] bfd multihop echo interface *interface-name* remote-ip *ip-*	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.

Step	Command	Description
	address [multiplier *multiplier-value* min-transmit-interval *minimum-transmit-interval-value* min-receive-interval *minimum-receive-interval-value*]	

Table 1389 Configure monitoring the BFD IPv6 multiple-hop session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track *track -id*	-
Configure monitoring the BFD session	bfd multihop control remote-ipv6 *ipv6-address* local-ipv6 *ipv6-address* [vrf *vrf-name*] [multiplier *multiplier-value* min-transmit-interval *minimum-transmit-interval-value* min-receive-interval *minimum-receive-interval-value*]	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.

10.9.2.3 Track Monitoring and Maintaining

Table 1390 Track monitoring and maintaining

Command	Description
show track object [*track-id* | brief]	Display the Track group information.

10.10 BFD

10.10.1 Overview

The BFD (Bidirectional Forwarding Detection) protocol is a set of standard and unified detection mechanism, used to detect and monitor the path in the network or IP route forwarding connection status fast. It provides one universal, standard, medium-

independent, and protocol-independent fast fault detection mechanism. It can fast detect the line fault between two devices for the upper-layer protocols, such as routing protocol and MPLS.

BFD can provide the fault detection on any type of path between the systems. One BFD session is set up based on the specific application demand. If multiple application protocols correspond to the same path, you can use one BFD session to detect.

The processing flow of the BFD protocol and the upper application protocol includes:

1. The upper application protocol sends the neighbor information (including peer IP address, local IP address, interface and so on) to the BFD protocol.
2. The BFD protocol queries whether there is the corresponding session. If no, create the corresponding session according to the received neighbor information and then the BFD session sends the BFD control packet to drive the running of the status machine. The BFD control packet completes the session via three times handshake mechanism, experiencing the transfer from Down to Init and from Init to Up. When setting up the session, the session parameters are negotiated, including the interval of sending packets and detection interval.
3. After the session is set up, send the detection packets periodically to detect the path status. If the BFD control packets of the peer device are not received within the detection interval, the BFD protocol regards that the path has fault and informs the fault information to the upper application protocol.
4. After the upper application protocol receives the fault report, inform the BFD protocol to delete the session when disabling or deleting the neighbor. If no other upper-layer protocol needs to detect the session link, delete the corresponding session.

According to the type of the detection path, it includes the single-hop path

detection and non-single-hop path detection.

10.10.2 BFD Function Configuration

Table 1391 BFD function configuration list

Configuration Task	
Configure the BFD basic functions	Configure the minimum sending interval of the single-hop BFD control packets
	Configure the minimum receiving interval of the single-hop BFD control packets
	Configure the detection timeout multiples of the single-hop BFD session
	Configure the authentication parameters of the single-hop BFD session
	Configure the minimum sending interval of the non-single-hop BFD control packets
	Configure the minimum receiving interval of the non-single-hop BFD control packets
	Configure the detection timeout multiples of the non-single-hop BFD session
	Configure the authentication parameters of the non-single-hop BFD session
	Configure the outgoing interface as the physical outgoing interface of the BFD session of the Tunnel interface

10.10.2.1 Configure BFD Basic Functions

Configuration Condition

Before configuring the BFD basic functions, first complete the following tasks:

- Configure the IP address of the interface, making the neighboring node network layer reachable
- Configure the upper-layer application associated with BFD

Configure Minimum Sending Interval of Single-hop BFD Control Packets

Table 1392 Configure the minimum sending interval of BFD control packets

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the minimum sending interval of BFD control packets	bfd min-transmit-interval *value*	Optional By default, the minimum sending interval of BFD control packets is 1000ms.

Note

- The actual sending interval of the peer BFD packets = MAX (minimum sending interval of the peer BFD control packets, the minimum receiving interval of the local BFD control packets)

Configure Minimum Receiving Interval of Single-hop BFD Control Packets

Table 1393 Configure the minimum receiving interval of the BFD control packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the minimum receiving interval of the BFD control packet	bfd min-receive-interval *value*	Optional By default, the minimum receiving interval of the BFD control packets is 1000ms.

Note

- The actual sending interval of the local BFD packets = MAX (minimum sending interval of the local BFD control packets, the minimum receiving interval of the peer BFD control packets)

Configure Detection Timeout Multiples of Single-hop BFD Session

Table 1394 Configure the detection timeout multiples of the BFD session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the detection timeout multiples of the BFD session	bfd multiplier *value*	Optional By default, the detection timeout multiples of the BFD session is 5.

Note

- To ensure the validity of the BFD session detection, be careful to configure the minimum of the BFD detection timeout multiples.
- Local BFD actual detection time = the detection timeout multiples of the peer BFD session × the actual sending interval of the peer BFD packet

Configure Authentication Parameters of Single-Hop BFD Session

Table 1395 Configure the authentication parameters of the single-hop BFD session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the authentication	bfd authentication key-*id* { { m-	Optional

Step	Command	Description
parameters of the single-hop BFD session	md5 | m-sha1 | m-sm3 | md5 | sha1 | sm3 } { 0 *plain-key* | 7 *cipher-key* } } | { simple { 0 *plain-password* | 7 *cipher-password* } }	By default, do not configure the authentication parameters of the single-hop BFD session.

Note

- After the BFD authentication function is enabled on the interface, it is only effective for single hop sessions based on the interface.
- In order to ensure that BFD authentication can take effect correctly, the authentication information of the interfaces at both ends of BFD session must be consistent.

Configure Minimum Sending Interval of Non-Single-hop BFD Control Packets

Table 1396 Configure the minimum sending interval of the non-single-hop BFD control packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the minimum sending interval of the non-single-hop BFD control packet	bfd non-single-hop min-transmit-interval *value*	Optional By default, the minimum sending interval of non-single-hop BFD control packets is 1000ms.

Note

- The actual sending interval of the local BFD packets = MAX (minimum sending interval of the local BFD control packets, the minimum receiving interval of the peer BFD control packets)
- After configuring the minimum receiving time interval of non-single hop BFD control packet, it will take effect for IPv4/IPv6 multi-hop session and MPLS LSP session. If the registration module specifies the minimum receiving time interval of non-single hop BFD control packet, it will take effect with the value specified by the module. If multiple registration modules specify the minimum receiving time interval of non-single hop BFD control packet of the same session at the same time, it will take effect with the specified minimum value.

Configure Minimum Receiving Interval of Non Single-hop BFD Control Packets

Table 1397 Configure the minimum receiving interval of the non-single-hop BFD control packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the minimum receiving interval of the non-single-hop BFD control packet	bfd non-single-hop min-receive-interval *value*	Optional By default, the minimum receiving interval of the non-single hop BFD control packets is 1000ms.

Note

- The actual sending interval of the peer BFD control packets = MAX (minimum sending interval of the peer BFD control packets, the minimum receiving interval of the local BFD control packets)
- After configuring the minimum sending time interval of non-single hop BFD control packet, it will take effect for IPv4/IPv6 multi-hop session

and MPLS LSP session. If the registration module specifies the minimum sending time interval of non-single hop BFD control packet, it will take effect with the value specified by the module. If multiple registration modules specify the minimum sending time interval of non-single hop BFD control packet of the same session at the same time, it will take effect with the specified minimum value.

Configure Detection Timeout Multiples of Non-Single-hop BFD Session

Table 1398 Configure the detection timeout multiples of the non-single-hop BFD session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the detection timeout multiples of the non-single-hop BFD session	bfd non-single-hop multiplier *value*	Optional By default, the detection timeout multiples of the non-single-hop BFD session is 5.

Note

- To ensure the validity of the BFD session detection, be careful to configure the minimum of the BFD detection timeout multiples.
- Local BFD actual detection time = the detection timeout multiples of the peer BFD session × the actual sending interval of the peer BFD packet
- After configuring the detection timeout multiple of non-single hop BFD sessions, it will take effect for IPv4/IPv6 multi hop sessions and MPLS LSP sessions. If the registration module specifies the detection timeout multiple of non-single hop BFD session, the value specified by the registration module takes effect. If multiple registration modules specify the detection timeout multiple of non-single hop BFD sessions of the

same session at the same time, the specified minimum value will take effect.

Configure Authentication Parameters of Non-Single-Hop BFD Session

Table 1399 Configure the authentication parameters of the non-single-hop BFD session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the authentication parameters of the non-single-hop BFD session	bfd non-single-hop authentication *key-id* { { m-md5 | m-sha1 | m-sm3 | md5 | sha1 | sm3 } { 0 *plain-key* | 7 *cipher-key* } } | { simple { 0 *plain-password* | 7 *cipher-password* } }	Optional By default, do not configure the authentication parameters of the non-single-hop BFD session.

Note

- After the non-single-hop BFD authentication function is enabled on the interface, it is effective for IPv4/IPv6 multi-hop session and MPLS LSP session.
- In order to ensure that BFD authentication can take effect correctly, the authentication information of the interfaces at both ends of non-single-hop BFD session must be consistent.

Configure Fast Detection Function of BFD Session

Table 1400 Configure the fast detection function of the BFD session

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the fast detection function of the BFD session	bfd fast-detect	Optional By default, the fast detection function of the BFD session is

Step	Command	Description
		disabled.

10.10.2.2 BFD Monitoring and Maintaining

Table 1401 BFD monitoring and maintaining

Command	Description
show bfd capability	Display the BFD capability information
show bfd discriminator	Display the BFD local discriminator value information
show bfd session	Display the information of the BFD IPv4 session
show bfd session ipv6	Display the information of the BFD IPv6 session
show bfd session mpls	Display the information of the BFD MPLS session
show bfd session summary	Display the summary information of the BFD session

10.10.3 BFD Typical Configuration Example

10.10.3.1 Configure BFD Basic Functions

Network Requirements

- Device 4 is a connected device that only transparently transmits data.
- Device1, Device2 and Device3 run OSPF protocol, and device1 and device3 are configured with BFD detection function.
- Modify BFD parameters. When the line between Device4 and Devcie3 fails, the service data between Device1 and Device3 can be switched in milliseconds.

Network Topology

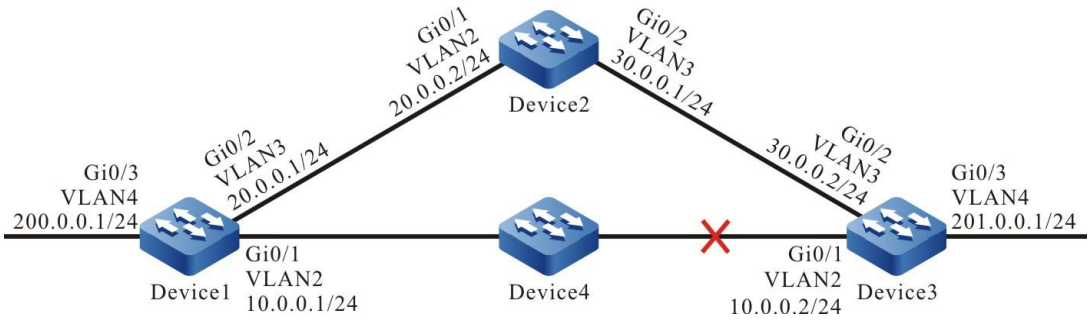


Figure 310 Networking of configuring BFD basic functions

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 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 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
```

#View 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
```

It can be seen that OSPF and BFD are linked successfully, the session is established normally, and the detection timeout is 5 seconds.

#View the routing table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

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
```

According to the routing table, route 201.0.0.0/24 preferably communicates with the line between Device1 and Device3.

Step 5: Configure the BFD parameters.

#Configure Device1, modify the minimum sending interval and minimum receiving interval of BFD control packets to 100ms, and the detection timeout multiple is 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 interval and minimum receiving interval of BFD control packets to 100ms, and the detection timeout multiple is 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.

#View 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 was negotiated

from the previous 5 seconds to 300 milliseconds.

#When the line between Device1 and Device3 fails, BFD will quickly detect the fault and notify OSPF. OSPF will switch the route to Device2 for communication and check the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external
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
```

Comparing the routing table in Step 3, we can see that the route 201.0.0.0/24 has been switched to Device2 for communication.

The BFD processing method on Device3 is similar to that of Device1.

10.11 EEP

10.11.1 Overview

EEP: embedded event platform, which is an extensible and customizable event detection and processing mechanism directly provided in the device. EEP provides a method for users to monitor specific events, obtain information and set actions when events occur.

10.11.2 EEP Function Configuration

Table 1402 EEP function configuration list

Configuration Task	
Configure EEP policy	Configure the EEP policy
Configure the EEP event	Configure EEP to bind none event
	Configure EEP to bind the timer event
	Configure EEP to bind TRACK event
Configure the EEP action	Configure the EEP action

10.11.2.1 Configure EEP Policy

Configuration Condition

None

Configure EEP Policy

The system can configure multiple EEP policies. Each EEP policy is independent of each other. Only one EEP event can be configured in an EEP policy, and up to 50 EEP actions can be configured.

EEP policy has three states: init, running and suspend:

- The EEP policy is created for the first time, and the status of the EEP policy is init.
- In the created EEP policy, configure EEP events and EEP actions. The status of EEP policy is changed to running. In this state, the EEP policy will execute the configured EEP actions successively after monitoring the configured EEP events.
- The user can suspend all configured EEP policies or a specified EEP policy through the command **event platform suspend** {**policy** *policy-name*}. The EEP policy status changes to suspend. In this state, the EEP policy will not execute the configured EEP action after monitoring the configured EEP event.

Table 1403 Configure the EEP policy

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create EEP policy	event platform applet *policy-name*	Mandatory
Suspend EEP policy	event platform suspend {policy *policy-name*}	Optional

10.11.2.2 Configure EEP Event

Configuration Conditions

Before configuring the EEP event, first complete the following task:

- Configure the EEP policy

Configure EEP to Bind None Event

Table 1404 Configure EEP to bind none event

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EEP policy configuration mode	event platform applet *policy-name*	-
Configure EEP to bind none event	event none	Mandatory

Note

- The EEP binds null events, and the EEP policy has no events to monitor. Therefore, the user can only trigger the EEP policy of binding null events to execute EEP actions through the command **event platform run** *policy-name*.

Configure EEP to Bind Timer Event

The timer events bound to EEP can be divided to four kinds of timer events:

- Absolute timer: The timer event is triggered when the specified time configured by the user arrives.
- Calendar timer: The timer event is triggered when the periodic time configured by the user arrives.
- Countdown timer: When the countdown time configured by the user arrives, the timer event is triggered.

- Watchdog timer: When the watchdog time configured by the user arrives, the timer event is triggered.

Table 1405 Configure EEP to bind the timer event

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EEP policy configuration mode	event platform applet policy-name	-
Configure EEP to bind the Absolute timer event	event timer absolute year month day hour:minute[:second]	Optional
Configure EEP to bind the Calendar timer event	event timer calendar { per-day hour:minute[:second] | per-hour minute | per-month day hour:minute[:second] | per-week week hour:minute[:second] }	Optional The value range of minute is 0-59. The value range of day is 1-28. The value range of week is 0-6, 0 indicates Sunday.
Configure EEP to bind the Countdown timer event	event timer countdown time-value	Optional The value range of time-value is 1-107374182, and the unit is second.
Configure EEP to bind the Watchdog timer event	event timer watchdog time-value	Optional The value range of time-value is 1-107374182, and the unit is second.

Configure EEP to Bind TRACK Event

Table 1406 Configure EEP to bind the TRACK event

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EEP policy configuration mode	event platform applet *policy-name*	-
Configure EEP to bind the	event track *track-id* {*up-*	Optional

TRACK event	*to-down*| *down-to-up*}	The value range of *track-id* is 1-500.

10.11.2.3 Configure EEP Actions

Table 1407 Configure the EEP actions

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the EEP policy configuration mode	event platform applet *policy-name*	-
Configure EEP to execute the command line actions	action *action-number* {cli-command *cli-command-string* | force-switchover | reload [master | slave] | syslog [msg *message-text* | priority *priority-value* msg *message-text*]}	Optional The value range of *action-number* is 1-1000.

Note

- When EEP policy executes command actions, execute the command line from small to large according to *action-number*.
- The command line ***cli-command-string*** is executed in configuration mode by default.

10. 11. 2. 4 EEP Monitoring and Maintaining

Table 1408 EEP monitoring and maintaining

Command	Description
show eep policy registered { detail | INEXIST-EVENT | NONE-EVENT | TIMER-EVENT | TRACK-EVENT }	View all EEP policy status information

10.11.3 EEP Typical Configuration Example

10.11.3.1 Configure EEP Policy to Associate PBR

Network Requirements

- OSPF protocol is running on all devices, and PBR is configured on Device1.
- By configuring PBR, PC can access server 2.2.2.2 through Device1 and Device2.
- By configuring EEP to associate PBR, when the interface between Device1 and Device2 goes down, EEP will quickly notify PBR to delete the next hop configuration, so that PC can access server 2.2.2.2 through Device1 and Device3; When the link between Device1 and Device2 returns to normal, EEP notifies PBR to add the next hop configuration to enable PC to access server 2.2.2.2 through Device1 and Device2.

Network Topology

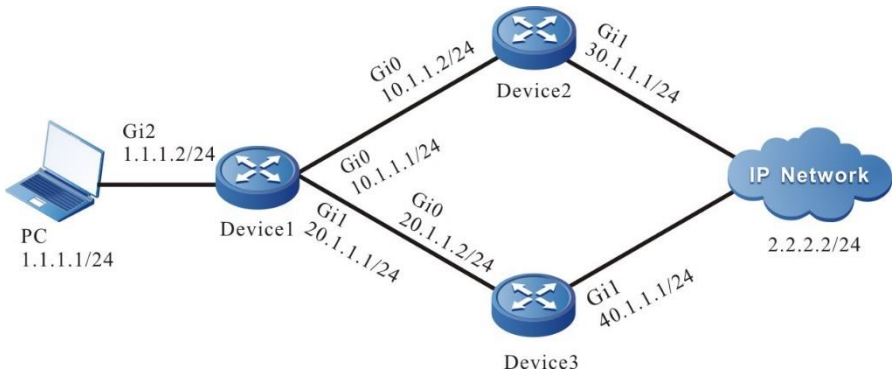


Figure 311 Networking of configuring EEP policy to associate with PBR

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the 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)#router-id 1.1.1.1
Device1(config-ospf)#network 1.1.1.0 0.0.255 area 0
Device1(config-ospf)#network 11.1.0 0.0.255 area 0
Device1(config-ospf)#network 21.1.0 0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device1(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 11.1.0 0.0.255 area 0
Device2(config-ospf)#network 31.1.0 0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device1(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 21.1.0 0.0.255 area 0
Device3(config-ospf)#network 41.1.0 0.0.255 area 0
Device3(config-ospf)#exit
```

#Check the routing table of Device1. You can see that there are two next hops to the 2.2.2.0/24 network.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.1.1.0/24 is directly connected, 22:14:53, gigabitethernet2
L   1.1.1.1/32 is directly connected, 22:14:53, gigabitethernet2
O   2.2.2.0/24 [110/3] via 11.1.2, 00:00:09, gigabitethernet0
              [110/3] via 21.1.2, 00:00:09, gigabitethernet1
C   11.1.0/24 is directly connected, 21:41:21, gigabitethernet0
L   11.1.1/32 is directly connected, 21:41:21, gigabitethernet0
C   21.1.0/24 is directly connected, 15:19:15, gigabitethernet1
L   21.1.1/32 is directly connected, 15:19:15, gigabitethernet1
O   31.1.0/24 [110/2] via 11.1.2, 18:55:36, gigabitethernet0
O   41.1.0/24 [110/2] via 21.1.2, 00:22:08, gigabitethernet1
C   127.0.0.0/8 is directly connected, 87:42:47, lo0
L   127.0.1/32 is directly connected, 87:42:47, lo0
```

#Configure Device1 and modify the cost value of the interface gigabitethernet0 to 100, so that the route to the 2.2.2.0/24 network preferably selects the gigabitethernet1 interface.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip ospf cost 100
Device1(config-if-gigabitethernet0)#exit
```

#View the route table of Device1.

```
Device1#show ip 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, E - IRMP, EX - IRMP external

C   1.1.1.0/24 is directly connected, 23:27:34, gigabitethernet2
L   1.1.1.1/32 is directly connected, 23:27:34, gigabitethernet2
O   2.2.2.0/24 [110/3] via 21.1.2, 01:12:50, gigabitethernet1
C   11.1.0/24 is directly connected, 22:54:03, gigabitethernet0
L   11.1.1/32 is directly connected, 22:54:03, gigabitethernet0
C   21.1.0/24 is directly connected, 16:31:57, gigabitethernet1
L   21.1.1/32 is directly connected, 16:31:57, gigabitethernet1
O   31.1.0/24 [110/3] via 21.1.2, 00:31:42, gigabitethernet0
O   41.1.0/24 [110/2] via 21.1.2, 01:34:50, gigabitethernet1
C   127.0.0.0/8 is directly connected, 88:55:28, lo0
L   127.0.1/32 is directly connected, 88:55:28, lo0
```

#View the path to the server 2.2.2.2 through the **traceroute** command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

 1    1 ms    1 ms    1 ms  1.1.1.2
 2   <1 ms   <1 ms   <1 ms  21.1.2

 n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

It can be seen that PC accesses server 2.2.2.2 through Device1 and Device3.

Step 3: On Device1, configure the policy routing.

#Configure ACL 1001, permitting PC to access the network 2.2.2.0/24.

```
Device1(config)#ip access-list extended 1001
Device1(config-ext-nacl)#permit ip any 2.2.2.0 0.0.255
```

```
Device1(config-ext-nacl)#exit
```

#Configure policy routing aaa, associate access control list 1001, and specify the next hop as 11.1.2.

```
Device1(config)#route-policy aaa permit 10
Device1(config-pbr)#match ip address acl 1001
Device1(config-pbr)#set ip next-hop 11.1.2
Device1(config-pbr)#exit
```

#View the information of the policy route aaa of Device1.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
    set ip next-hop 11.1.2
```

Step 4: Apply policy routing.

#On the interface gigabitethernet2 of Device1, apply the policy routing aaa.

```
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)#ip policy aaa
Device1(config-if-gigabitethernet2)#exit
```

#On the PC, view the path to the server 2.2.2.2 via the command Traceroute.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

 1    1 ms    1 ms    1 ms  1.1.1.2
 2    <1 ms   <1 ms   <1 ms  11.1.2

 n    <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

You can see that after the policy routing is applied to the interface gigabitethernet2, the PC accesses the server 2.2.2.2 through Device1 and Device2.

Step 5: Configure EEP policy to associate PBR.

#Configue TRACK 1 to monitor the status of the interface gigabitethernet 0.

```
Device1(config)#track 1
Device1(config-track)#interface gigabitethernet0 line-protocol
```

```
Device1(config-track)#exit
```

#Configure EEP policy e1 on Device1, bind track group 1, monior the status of interface gigabitethernet0, and notify PBR to delete the corresponding next hop configuration when Device1 interface gigabitethernet0 is down.

```
Device1(config)#event platform applet e1
Device1(config-eep)#event track 1 up-to-down
Device1(config-eep)#action 1 cli-command route-policy aaa permit 10
Device1(config-eep)#action 2 cli-command no set ip next-hop 11.1.2
Device1(config-eep)#exit
```

#Configure EEP policy e2 on Device1, bind track group 1, monior the status of interface gigabitethernet0, and notify PBR to delete the corresponding next hop configuration when Device1 interface gigabitethernet0 is up.

```
Device1(config)#event platform applet e2
Device1(config-eep)#event track 1 down-to-up
Warning:
Configuring event track 1 down-to-up is risky, are you sure to configure?(Yes/No)yes
Device1(config-eep)#action 1 cli-command route-policy aaa permit 10
Device1(config-eep)#action 2 cli-command set ip next-hop 11.1.2
Device1(config-eep)#exit
```

Step 6: Check the result.

#When interface gigabitethernet0 of Device1 is down, EEP will quickly notify PBR to delete the next hop configuration, and PC will access server 2.2.2.2 through Device3.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
```

#View the path to the server 2.2.2.2 through the traceroute command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

 1    1 ms    1 ms    1 ms  1.1.1.2
 2    <1 ms   <1 ms   <1 ms  21.1.2

 n    <1 ms   <1 ms   <1 ms  2.2.2.2
```

```
Trace complete.
```

You can see that after the interface gigabitethernet2 is down, the PC accesses the server 2.2.2.2 through Device1 and Device3.

#When the interface gigabitethernet0 of Device1 is up, EEP will notify PBR to add the next hop configuration, and PC will access server 2.2.2.2 through Device2.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
    set ip next-hop 11.1.2
```

#View the path to the server 2.2.2.2 through the traceroute command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

 1    1 ms    1 ms    1 ms  1.1.1.2
 2   <1 ms   <1 ms   <1 ms  11.1.2

 n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

You can see that after the interface gigabitethernet2 is up, the PC accesses server 2.2.2.2 through Device1 and Device2.

10.12 ERPS

10.12.1 Overview

STP (Spanning Tree Protocol) is generally used for network reliability in Ethernet L2 networks, but STP (Spanning Tree Protocol) usually converges in seconds, and the convergence time is longer when the network diameter is larger. In order to shorten the convergence time and eliminate the influence of the network size, ERPS (Ethernet Ring Protection Switching) technology came into being. ERPS (Ethernet Ring Protection Switching) is a L2 protocol standard defined by ITU-T, and the protocol standard number is ITU-T G.8032/Y1344, also known as G.8032. G. 8032 is a link layer

technology of Ethernet ring network with high reliability and stability. It can prevent the broadcasting storm caused by the data loop when the Ethernet ring network is intact. When the link of the Ethernet ring network fails, it can quickly restore the communication path between the nodes on the ring network, and has a high convergence speed. Meanwhile, if the equipment of the manufacturers in the ring network supports the protocol, they can communicate with each other.

ERPS related concepts:

- ERPS (Ethernet Ring Protection Switching) Ring: ERPS Ring is the basic unit of the ERPS protocol. It consists of a group of the interconnected network devices with the same control VLAN (Virtual Local Area Network). ERPS rings are divided into main rings and sub-rings. The main rings are closed rings and the sub-rings are non-closed rings. The attributes of the main and sub-rings are determined by the user.
- Port role: There are three types of port roles specified in the ERPS protocol: RPL owner port, RPL neighbor port and common port, among which RPL neighbor port type is only supported by ERPSv2 version.
- RPL owner port: An ERPS ring has only one RPL owner port, which is specified by the user configuration. ERPS protocol prevents the link from generating loops by blocking the forwarding status of the RPL owner port. 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. Normally, both RPL owner ports and RPL neighbor ports are blocked to prevent loops. When ERPS ring network fails, RPL owner port and RPL neighbor port will be opened.
- Ordinary port: In ERPS ring, all ports except RPL owner port and RPL neighbor port are ordinary ports. Ordinary ports are responsible for monitoring their own direct-connected link status, and timely notifying other node ports of link status changes.

- ERPS Controls VLAN: Used to transmit ERPS protocol packets. The control VLAN is specified by the user. The VLAN used as ERPS control VLAN cannot be used by other services. The control VLAN of each ERPS loop is different.
- ERPS data instance: The data instance of data VLAN mapping that needs the ERPS ring protection.

10.12.2 ERPS Function Configuration

Table 1409 ERPS function configuration list

Configuration Tasks	
Configure the ERPS ring	Configure the ERPS ring
	Enable the ERPS protocol
Configure the ERPS ring timer	Configure the ERPS ring timer
Configure the ERPS network optimization	Configure the switching mode of the ERPS port blocking
	Clear the blocking points of the ERPS configuration
	Configure the notification of the ERPS topology change
	Configure the ERPS TC limitation function
Configure ERPS to associate with CFM	Configure ERPS to associate with CFM

10.12.2.1 Configure the ERPS Ring

When configuring the ERPS ring, it is necessary to configure the ports on each node that access the ERPS ring and the nodes on the ring.

Configuration Conditions

Before configuring the ERPS ring, first complete the following tasks:

- Create one control VLAN
- Close the ring network protocol of the ring ports
- Configure the ring port as the trunk mode

- Add the ring ports to the control VLAN of the ring
- Configure the MSTP instance and the mapping relation of the contained VLANs

Configure the ERPS Ring

Configure the basic functions of the ERPS ring.

Table 1410 Configure the ERPS ring

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create one ERPS ring	erps ring *ring-id*	Mandatory By default, do not create one ERPS ring, and the value range of the ring is 1-64.
Configure the ERPS ring control VLAN	control vlan *vlan-id*	Mandatory By default, do not configure the control VLAN of the ERPS ring.
Configure the ERPS ring data instance	instance *instance-list*	Mandatory By default, do not configure the ERPS data instance.
Configure the ERPS ring port PORT0	port0 { interface *interface-name* | interface link-aggregation link-aggregation-id } [rpl { owner | neighbour }]	Mandatory By default, do not configure the ERPS port0. rpl owner: Indicate that the port is the owner port of RPL rpl neighbor: Indicate that the port is the neighbor port of RPL. If not configuring rpl, indicate that the port is the ordinary port.
Configure the ERPS ring port	port1 { interface *interface-name* |	Mandatory

PORT1	interface link-aggregation link-aggregation-id } [rpl { owner | neighbour }]	By default, do not configure the ERPS port1. rpl owner: Indicate that the port is the owner port of RPL rpl neighbor: Indicate that the port is the neighbor port of RPL. If not configuring rpl, indicate that the port is the ordinary port.
Configure the version information of the ERPS ring	version { *v1* | *v2* }	Optional By default, the version is V2.
Configure the mel value of the ERPS ring packet	mel *level-id*	Optional By default, the mel value is 7, and the value range is 0-7.
Configure the ERPS ring is the sub ring	sub-ring	Optional By default, the ERPS ring is the main ring.
Configure the ERPS ring to the non-switchback mode	revertive disable	Optional By default, the ERPS is the switchback mode.
Configure the virtual channel of the ERPS sub ring	virtual-channel enable	Optional By default, ERPS is the non-virtual channel.

Note

- ERPS control VLAN can only be used for transmitting the ERPS protocol packets, not for other services. All nodes in the same ERPS ring need to configure the same Mel value.
- Subring virtual channel is not recommended in the intersecting ring networking environment.

Enable the ERPS Protocol

After the above configuration is complete, use the command to enable the ERPS protocol.

Table 1411 Enable the protocol on the ERPS ring

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ERPS configuration mode	erps ring *ring-id*	-
Enable the ERPS protocol	erps enable	Mandatory By default, the ring does not enable the ERPS protocol.

10.12.2.2 Configure the ERPS Ring Timer

Configuration Conditions

Before configuring the ERPS timer, first complete the following task:

- Configure the ERPS ring

Configure ERPS Ring Timer

In order to prevent network oscillation, ERPS ring timer will be enabled to reduce the interruption time of traffic after the failure of the node equipment or link in ERPS ring recovers.

Table 1412 Configure the ERPS timer

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ERPS configuration mode	erps ring *ring-id*	-
Configure the Guard timer of the ERPS ring	guard-timer *time-value*	Mandatory By default, the timeout of the Guard timer is 500ms, and the

		range of the Guard timer is 10-2000ms.
Configure the Hold-off timer of the ERPS ring	holdoff-timer *time-value*	Mandatory By default, the timeout of the hold-off timer is 0ms, and the range of the hold-off timer is 0-10000ms.
Configure the WTR timer of the ERPS ring	wtr-timer *time-value*	Mandatory By default, the timeout of the WTR timer is 5 minutes, and the range of the WTR timer is 1-12 minutes.

10.12.2.3 Configure ERPS Network Optimization

Configuration Conditions

Before configuring the ERPS network optimization, first complete the following task:

- Configure the ERPS ring

Configure the Switching Mode of the ERPS Port Blocking

Since the bandwidth of the link where the RPL owner port is located may be able to carry more user traffic, it is possible to consider blocking the link with low bandwidth so that the user traffic can be transmitted back to RPL.

Table 1413 Configure the switching mode of the ERPS port blocking

Step	Command	Description
Configure the switching mode of the ERPS port blocking	erps ring *ring-id* { interface *interface-name* | interface link-aggregation link-aggregation-id } switch { force | manual }	Mandatory By default, do not configure the switching mode of the blocking point of the ERPS ring port.

Clear the Blocking Points of ERPS Configuration

Clear the blocking points of the ERPS ring configuration.

Table 1414 Clear the blocking points of the ERPS configuration

Step	Command	Description
Clear the blocking points of the ERPS configuration	clear erps ring *ring-id*	Mandatory

Configure the Notification of ERPS Topology Change

When the topology of the ERPS loop changes and the superior L2 network is not notified in time, the MAC address table of the superior L2 network still retains the MAC address table entries before the downstream network topology changes, which will cause the interruption of the user traffic. In order to ensure the normal communication of user traffic, it is necessary to select the notification object of the ERPS loop according to the actual network of the user.

Table 1415 Configure the notification of the ERPS ring topology change

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ERPS configuration mode	erps ring *ring-id*	-
Configure the notification of the ERPS ring topology change	tc-notify erps ring *ring-list*	Mandatory By default, do not notify the change of the ERPS topology.

Configure ERPS TC Limit Function

The frequent notification of topology change will lead to the decline of CPU processing capacity, and the flush-FDB packets frequently refreshed on the ERPS ring occupy network bandwidth. In order to avoid this situation, it is necessary to suppress the notification packets of topology change. By configuring the protection interval of ERPS topology change and the maximum threshold of the topology change packets processed in the protection interval of the topology change, suppress the notification of topology change and avoid deleting the MAC address entries and ARP entries frequently, so as to protect the equipment.

Table 1416 Configure the ERPS TC limit function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ERPS configuration mode	erps ring *ring-id*	-
Configure enabling the TC limit of the ERPS topology change	tc-limit enable	Mandatory By default, do not enable the TC limit function.
Configure the interval of the TC limit of the ERPS topology change	tc-limit interval *interval-value*	Optional The default interval is 2s, and the value range is 1-500s.
Configure the threshold of the TC limit of the ERPS topology change	tc-limit threshold *threshold-value*	Optional The default value is 3, and the value range is 1-64.

10.12.2.4 Configure ERPS to Link with CFM

Configuration Conditions

Before configuring ERPS to link with CFM (Connectivity Fault Management), first complete the following task:

- Configure the basic functions of ERPS
- Configure the CFM function

Configure ERPS to Link with CFM

After configuring the Ethernet CFM linkage function on the ring port added to the ERPS ring, you can speed up the fault detection, realizing the fast convergence of the topology and reducing the interruption time of the traffic.

Table 1417 Configure ERPS to link with CFM

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2 Ethernet interface	interface *interface-name*	Either

configuration mode		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	interface link-aggregation link-aggregation-id	
Configure ERPS to link with CFM	erps ring *ring-id* track cfm domain *domain-name* service-instance *ser-name* mep *mep-id* remote-mep *rmep-id*	Mandatory By default, the port does not link with CFM.

10.12.2.5 ERPS Monitoring and Maintaining

Table 1418 ERPS monitoring and maintaining

Command	Description
clear erps [ring *ring-id*] statistics	Clear the ERPS related statistics information
show erps [ring *ring-id*] config	Display the ERPS configuration information
show erps [ring *ring-id*] detail	Display the ERPS detailed information
show erps [ring *ring-id*] statistics	Display the ERPS statistics information

10.12.3 ERPS Typical Configuration Example

10.12.3.1 Configure ERPS Basic Functions

Network Requirements

- All Devices are in one L2 network.
- All devices enable ERPS, and adopt ERPS to cut the link rings in the network.

Network Topology

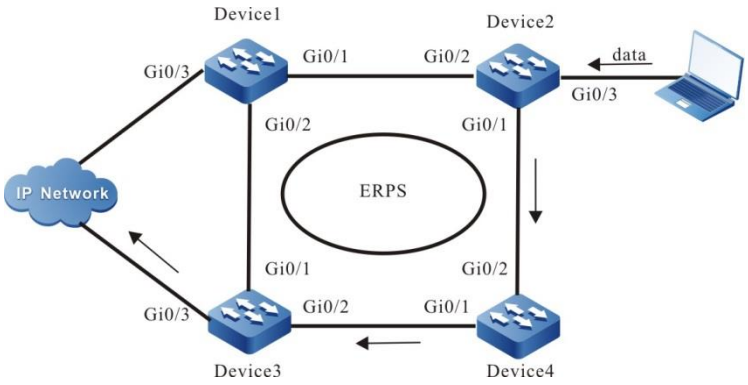


Figure 312 Configure ERPS basic functions

Configuration Steps

Step 1: Configure vlan and port link type.

#On Device1, create VLAN2, VLAN100-VLAN200 respectively, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, vlan100-VLAN200 to pass. Disable the spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/2)# switchport mode trunk
Device1(config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/2)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/2)# no spanning-tree enable
```

```
Device1(config-if-gigabitethernet0/2)#end
```

#On Device2, create VLAN2, VLAN100-VLAN200 respectively, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, vlan100-VLAN200 to pass. Disable the spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device2 (config-if-gigabitethernet0/1)#exit
Device2 (config)# interface gigabitethernet 0/2
Device2 (config-if-gigabitethernet0/2)# switchport mode trunk
Device2 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device2 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device2 (config-if-gigabitethernet0/2)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device2 (config-if-gigabitethernet0/2)#end
```

#On Device3, create VLAN2, VLAN100~VLAN200 respectively, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, vlan100-VLAN200 to pass. Disable the spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
```

```
Device3 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device3 (config-if-gigabitethernet0/1)#exit
Device3 (config)# interface gigabitethernet 0/2
Device3 (config-if-gigabitethernet0/2)# switchport mode trunk
Device3 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device3 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device3 (config-if-gigabitethernet0/2)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device3 (config-if-gigabitethernet0/2)#end
```

#On Device4, create VLAN2, VLAN100-VLAN200 respectively, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, vlan100-VLAN200 to pass. Disable the spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4 (config-if-gigabitethernet0/1)# no spanning-tree enable
Device4 (config-if-gigabitethernet0/1)#exit
Device4 (config)# interface gigabitethernet 0/2
Device4 (config-if-gigabitethernet0/2)# switchport mode trunk
Device4 (config-if-gigabitethernet0/2)# no switchport trunk allowed vlan all
Device4 (config-if-gigabitethernet0/2)# switchport trunk allowed vlan add 2,100-200
Device4 (config-if-gigabitethernet0/2)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4 (config-if-gigabitethernet0/2)# no spanning-tree enable
Device4 (config-if-gigabitethernet0/2)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance 1 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 instance 1 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 instance 1 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 instance 1 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
```

Step 3: Configure ERPS.

#On Device1, configure ERPS ring1, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the owner port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable ERPS function of ring1.

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/2
Device2(config-erps1)# port1 interface g0/1
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 control VLAN of ring1, configure gigabitethernet0/1 as the neighbor port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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 control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2

as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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 netwotk topology becomes stable, query the ERPS information of the Device, and 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 status of at least one point in the ring network is down. Otherwise, it will cause loop.

10.12.3.2 Configure ERPS Load

Network Requirements

- All devices are in one L2 network.
- The data traffic of data1 is transmitted via device2-device1, and the data traffic of Data2 is transmitted via device4-device3, realizing the load balance and providing the link backup.

Network Topology

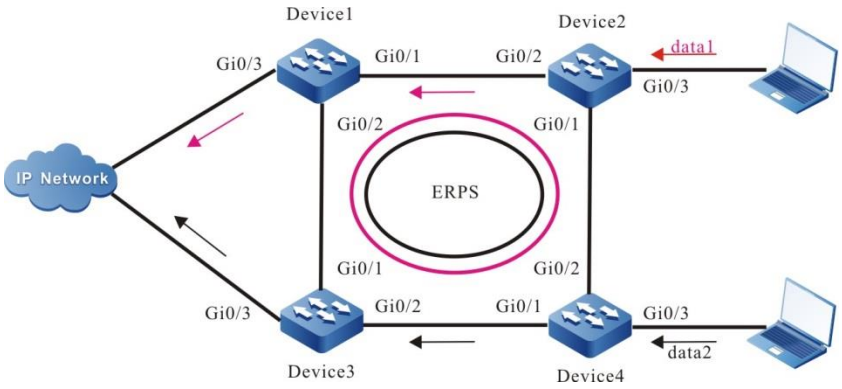


Figure 313 Configure ERPS load

Configuration Steps

Step 1: Configure vlan and port link type.

#On Device1, create VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400 to pass. Disable spanning tree and storm suppression on the port.

```
Device1#configure terminal
Device1(config)#vlan 2-3,100-200,300-400
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)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
```

```
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400 to pass. Disable spanning tree and storm suppression on the port.

```
Device2#configure terminal
Device2(config)# vlan 2-3,100-200,300-400
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)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400 to pass. Disable spanning tree and storm suppression on the port.

```
Device3#configure terminal
Device3(config)# vlan 2-3,100-200,300-400
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)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#end
```

#On Device4, create VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2-VLAN3, VLAN100-VLAN200, and VLAN300-VLAN400 to pass. Disable spanning tree and storm suppression on the port.

```
Device4#configure terminal
Device4(config)# vlan 2-3,100-200,300-400
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance 1 to map vlan100-200, configure MST instance 2 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 instance 1 to map vlan100-200, configure MST instance 2 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 instance 1 to map vlan100-200, configure MST instance 2 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 instance 1 to map vlan100-200, configure MST instance 2 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/1 as the normal port of ring2, configure gigabitethernet0/2 as the normal port of ring2, configure instance 2 as data VLAN of ring2, and enable the ERPS function of ring2.

```
Device1# configure terminal
Device1(config)#erps ring 2
Device1(config-erps2)# control vlan 3
Device1(config-erps2)# port0 interface g0/1
Device1(config-erps2)# port1 interface g0/2
Device1(config-erps2)# instance 2
Device1(config-erps2)# erps enable
Device1(config-erps2)# 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the owner port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/1 as the neighbor port of ring2, configure gigabitethernet0/2 as the normal port of ring2, configure instance 2 as data VLAN of ring2, and enable the ERPS function of ring2.

```
Device2# configure terminal
Device2(config)#erps ring 2
Device2(config-erps2)# control vlan 3
Device2(config-erps2)# port0 interface g0/1 rpl neighbor
Device2(config-erps2)# port1 interface g0/2
Device2(config-erps2)# instance 2
Device2(config-erps2)# erps enable
Device2(config-erps2)# 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/1 as the neighbor port of ring2, configure gigabitethernet0/2 as the normal port of ring2, configure instance 2 as data VLAN of ring2, and enable the ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps2)# control vlan 3
Device3(config-erps2)# port0 interface g0/1
Device3(config-erps2)# port1 interface g0/2
Device3(config-erps2)# instance 2
Device3(config-erps2)# erps enable
Device3(config-erps2)# 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the neighbor port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/1 as the normal port of ring2, configure gigabitethernet0/2 as the owner port of ring2, configure instance 2 as data VLAN of ring2, and enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps2)# control vlan 3
Device4(config-erps2)# port0 interface g0/1
Device4(config-erps2)# port1 interface g0/2 rpl owner
Device4(config-erps2)# instance 2
Device4(config-erps2)# erps enable
Device4(config-erps2)# 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 becomes stable, query the ERPS information of the Device, and take device2 as an example.

#Query 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     :  2  vlans mapped : 300-400
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

- When loading, multiple logical rings on one physical ring cannot be configured with the same data instance.

10.12.3.3 Configure ERPS Intersected Ring

Network Requirements

- All devices are in one L2 network.
- Device1-device2-device4-device3 and device3-device5-device6-device4 form two physical loops respectively, and all devices enable ERPS to the link loop.

Network Topology

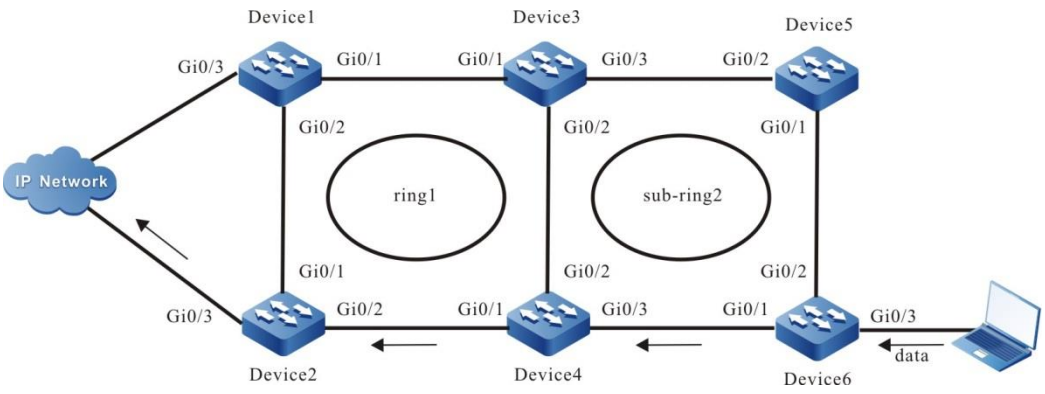


Figure 314 Configure ERPS intersected ring

Configuration Steps

Step 1: Configure vlan and port link type.

#On Device1, create VLAN2, and VLAN100-VLAN200, and configure the link

type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, and VLAN100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device1(config-if-gigabitethernet0/1)# no storm-control broadcast
Device1(config-if-gigabitethernet0/1)# no storm-control multicast
Device1(config-if-gigabitethernet0/1)# no spanning-tree enable
Device1(config-if-gigabitethernet0/1)#end
```

#On Device2, create VLAN2, and VLAN100-VLAN200, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, and VLAN100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
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)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device2(config-if-gigabitethernet0/1)# no storm-control broadcast
Device2(config-if-gigabitethernet0/1)# no storm-control multicast
Device2(config-if-gigabitethernet0/1)# no spanning-tree enable
Device2(config-if-gigabitethernet0/1)#end
```

#On Device3, create VLAN2-VLAN3, and VLAN100-VLAN200, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, and VLAN100-VLAN200 to pass. Configure the link type of port gigabitethernet0/3 as Trunk, permitting the services of VLAN3, vlan100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
Device3#configure terminal
Device3(config)#vlan 2-3,100-200
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 2,100-200
Device3(config-if-gigabitethernet0/1)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device3(config-if-gigabitethernet0/1)# no storm-control broadcast
```

```
Device3(config-if-gigabitethernet0/1)# no storm-control multicast
Device3(config-if-gigabitethernet0/1)# no spanning-tree enable
Device3(config-if-gigabitethernet0/1)#exit
```

#On Device4, create VLAN2-VLAN3, and VLAN100-VLAN200, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN2, and VLAN100-VLAN200 to pass. Configure the link type of port gigabitethernet0/3 as Trunk, permitting the services of VLAN3, vlan100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
Device4#configure terminal
Device4(config)#vlan 2-3,100-200
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device4(config-if-gigabitethernet0/1)# no storm-control broadcast
Device4(config-if-gigabitethernet0/1)# no storm-control multicast
Device4(config-if-gigabitethernet0/1)# no spanning-tree enable
Device4(config-if-gigabitethernet0/1)#exit
```

#On Device5, create VLAN3, and VLAN100-VLAN200, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN3, and VLAN100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
Device5#configure terminal
Device5(config)#vlan 3,100-200
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)# no storm-control unicast
Device5(config-if-gigabitethernet0/1)# no storm-control broadcast
Device5(config-if-gigabitethernet0/1)# no storm-control multicast
Device5(config-if-gigabitethernet0/1)# no spanning-tree enable
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)# no storm-control unicast
Device5(config-if-gigabitethernet0/1)# no storm-control broadcast
Device5(config-if-gigabitethernet0/1)# no storm-control multicast
Device5(config-if-gigabitethernet0/1)# no spanning-tree enable
Device5(config-if-gigabitethernet0/1)#end
```

#On Device6, create VLAN3, and VLAN100-VLAN200, and configure the link type of ports gigabitethernet0/1 and gigabitethernet0/2 as Trunk, permitting the services of VLAN3, and VLAN100-VLAN200 to pass. Disable spanning tree and storm suppression on the port.

```
Device6#configure terminal
Device6(config)#vlan 3,100-200
Device6(config)# interface gigabitethernet 0/1
Device6(config-if-gigabitethernet0/1)#shutdown
Device6(config-if-gigabitethernet0/1)# switchport mode trunk
Device6(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device6(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device6(config-if-gigabitethernet0/1)# no storm-control unicast
Device6(config-if-gigabitethernet0/1)# no storm-control broadcast
Device6(config-if-gigabitethernet0/1)# no storm-control multicast
Device6(config-if-gigabitethernet0/1)# no spanning-tree enable
```

```
Device6(config-if-gigabitethernet0/1)#exit
Device6(config)# interface gigabitethernet 0/2
Device6(config-if-gigabitethernet0/1)# switchport mode trunk
Device6(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device6(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device6(config-if-gigabitethernet0/1)# no storm-control unicast
Device6(config-if-gigabitethernet0/1)# no storm-control broadcast
Device6(config-if-gigabitethernet0/1)# no storm-control multicast
Device6(config-if-gigabitethernet0/1)# no spanning-tree enable
Device6(config-if-gigabitethernet0/1)#end
```

Step 2: Configure the MST instance.

#On Device1, configure MST instance 1 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 instance 1 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 instance 1 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 instance 1 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 instance 1 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 instance 1 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the owner port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the neighbor port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 as data VLAN of ring1, and enable 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/3 as the normal port of ring2, configure instance 1 as data VLAN of ring2, configure ring2 as sub-ring, and enable ERPS function of ring2.

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps2)# control vlan 3
Device3(config-erps2)# port0 interface g0/3
Device3(config-erps2)# instance 1
Device3(config-erps2)# sub-ring
Device3(config-erps2)# erps enable
Device3(config-erps2)# 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, configures vlan2 as control VLAN of ring1, configure gigabitethernet0/1 as the normal port of ring1, configure gigabitethernet0/2 as the normal port of ring1, configure instance 1 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/3 as the normal port of ring2, configure instance 1 as data VLAN of ring2, configure ring2 as sub-ring, and enable ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps2)# control vlan 3
Device4(config-erps2)# port0 interface g0/3
Device4(config-erps2)# instance 1
Device4(config-erps2)# sub-ring
Device4(config-erps2)# erps enable
Device4(config-erps2)# 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/2 as the normal port of ring2, configure gigabitethernet0/1 as the owner port of ring2, configure instance 1 as data VLAN of ring2, configure ring2 as sub-ring, and enable ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps2)# control vlan 3
Device4(config-erps2)# port0 interface g0/1 rpl owner
Device4(config-erps2)# port0 interface g0/2
```

```
Device4(config-erps2)# instance 1
Device4(config-erps2)# sub-ring
Device4(config-erps2)# erps enable
Device4(config-erps2)# 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, configures vlan3 as control VLAN of ring2, configure gigabitethernet0/2 as the neighbor port of ring2, configure gigabitethernet0/1 as the normal port of ring2, configure instance 1 as data VLAN of ring2, configure ring2 as sub-ring, and enable the ERPS function of ring2.

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps2)# control vlan 3
Device4(config-erps2)# port0 interface g0/1
Device4(config-erps2)# port0 interface g0/2 rpl neighbour
Device4(config-erps2)# instance 1
Device4(config-erps2)# sub-ring
Device4(config-erps2)# erps enable
Device4(config-erps2)# 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 becomes stable, query the ERPS information of the Device, and take device3 as an example.

#Query the ERPS information of Device3.

```
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

Device3# 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

11 Network Management and Monitoring

11.1Network Test and Fault Diagnosis

11.1.1 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.

11.1.2 Network Test and Fault Diagnosis Application

Table 1419 Application list of network test and fault diagnosis

Application functions	
Ping function	ping
	ping ip
	Interactive ping
	groupping
Traceroute function	traceroute
	Interactive traceroute
System debugging function	System debugging

11.1.2.1 Ping Function

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 Condition

None

Ping

Table 1420 ping

Step	Command	Description
Check whether the specified destination address is reachable	ping [vrf vrf-name] {[ip host-name | ip-address] | [ipv6 host-name | ipv6-address] | host-name | ip-address | ipv6-address } [-l packet-length] [-w wait-time] [-n packet-number | -t] [-f] [-h]	Mandatory

Interactive ping

If you need to use loose source route, strict source route, record route, record timestamp and other options, or you need to know the maximum ICMP packet size supported by the peer device, you can use the interactive ping to achieve.

Table 1421 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 | ipv6]	Optional By default, Use the IPv4 protocol.
Configure the destination IP address or host name	Target IP address or hostname:{ *ip-address* | *host-name* }	Mandatory
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.

Step	Command	Description
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. Only IPv4 protocol supports the command. After enabling the extended option, the command can be configured. 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. Only IPv4 protocol supports the command. After enabling the extended option, the command can be configured. By default, do not set the DF flag, permitting fragment.

Step	Command	Description
Configure the extended option, validating the data content of the response packet	Validate reply data? [no]:[yes | no]	Optional. Only IPv4 protocol supports the command. 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, only IPv4 protocol supports the command. 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, only IPv4 protocol supports the command. By default, scanning the sent packet is disabled.
Configure the start value of the scanning	Sweep min size [36]:[*min-szie*]	Optional, only IPv4 protocol supports the command. 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, only IPv4 protocol supports the command.

Step	Command	Description
		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, only IPv4 protocol supports the command. After enabling scanning the sent packet, the command can be configured. By default, the scanning incremental value is 1.

Groupping

The device supports sending multiple ICMP echo requests at one time, and gets more accurate network connection status according to the number of ICMP reply packets returned by the destination host.

Table 1422 groupping

Step	Command	Description
Send multiple groups of ICMP request packets, checking whether the destination address is reachable	groupping [vrf *vrf-name*] { *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”.

11.1.2.2 Traceroute Function

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 Condition

None

Traceroute

Table 1423 traceroute

Step	Command	Description
View the gateways passed by the packet from the source to the destination	traceroute [vrf *vrf-name*] {{ip *host-name* | *ip-address*} | {ipv6 *host-name* | *ipv6-address*} | *host-name* | *ip-address* | *ipv6-address* } [-f start-ttl] [-w wait-time] [-m max-ttl] [-s source] [-l packet-length] [-p dest-port] [-h]	Mandatory

Interactive traceroute

Table 1424 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

Step	Command	Description
		traceroute interactive mode.
Configure the network protocol type	Protocol [ip]:[ip | ipv6]	Optional By default, Use 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, record route, record timestamp, display details	Loose, Strict, Record, Timestamp, Verbose[none]:[l | s] [r / t / v]	Optional, only IPv4 protocol supports the command. By default, do not configure the option.

11.1.2.3 System Debugging Function

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 Condition

None

System Debugging

Table 1425 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 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.

11.1.2.4 Monitoring and Maintaining of Network Test and Fault Diagnosis

Table 1426 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.

11.1.3 Typical Configuration Example of Network Test and Fault Diagnosis

11.1.3.1 Ping Application

Network Requirement

- Device1 fails to log into Device3 by telnetting IP address and we need to confirm whether the IP route between Device1 and Device3 is reachable.
- Device1 fails to log into Device3 by telnetting IPv6 address and we need to

confirm whether the IPv6 route between Device1 and Device3 is reachable.

Network Topology

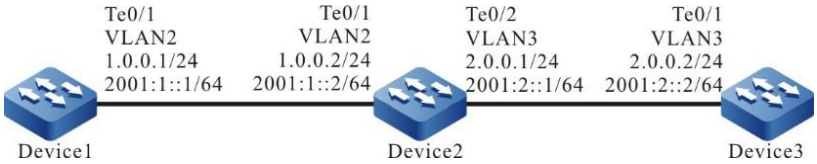


Figure 315 ping application networking

Configuration Steps

Step 1: Configure the IP address and IPv6 global unicast address of the interface. (Omitted)

Step 2: Use the ping command to view whether the route between Device1 and Device3 is reachable.

#View whether Device1 can ping the IP address 2.0.0.2 of Device3.

```
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).
```

#View whether Device1 can ping the IPv6 address 2001:2::2 of Device3.

```
Device1#ping 2001:2::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

Step 3: Use the ping command to view whether the route between Device1 and Device2 is reachable.

#View whether Device1 can ping the IP address 1.0.0.2 of Device2.

```
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.
```

#View whether Device1 can ping the IPv6 address 2001:1::2 of Device2.

```
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 = 0/0/0 ms.
```

Step 4 Use the ping command to view whether the route between Device2 and Device3 is reachable.

#View whether Device2 can ping IP address 2.0.0.2 of Device3.

```
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.
```

#View whether Device2 can ping the IPv6 address 2001:2::2 of Device3.

```
Device2#ping 2001:2::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/176/883 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** and **debug ipv6 icmp** commands to view whether the contents of the ICMP packet and ICMPv6 packet are correct. We also can use traceroute described in the next section to confirm the faulty network node.

11.1.3.2 Traceroute Application

Network Requirement

- Device1 fails to log into Device3 by telnetting IP address and we need to confirm whether the IP route between Device1 and Device3 is reachable. If the route is unreachable, we need to confirm the faulty network node.
- Device1 fails to log into Device3 by telnetting IPv6 address and we need to confirm whether the IPv6 route between Device1 and Device3 is reachable. If the route is unreachable, we need to confirm the faulty network node.

Network Topology

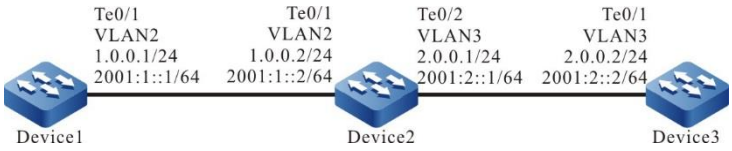


Figure 316 Traceroute application networking

Configuration Steps

Step 1: Configure the IP address and IPv6 global unicast address of the interface. (Omitted)

Step 2: Use the **traceroute** command to confirm the fault point between Device1 and Device3.

#Use the **traceroute** command to confirm the IPv4 fault point between Device1 and Device3.

```
Device1#traceroute  2.0.0.2
 Type (ctrl + shift + 6) 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
```

#Use the traceroute command to confirm the IPv6 fault point between Device1 and Device3.

```
Device1#traceroute 2001:2::2

Type (ctrl + shift + 6) to abort.Tracing the route to 2001:2::2 , min ttl = 1, max ttl = 30 .

1  2001:1::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** and **debug ipv6 icmp** command to view whether the contents of the ICMP packet and ICMPv6 packet are correct. We also can use ping described in the last section to detect the connection between Device2 and Device3

11.2Keepalive Gateway

11.2.1 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.

11.2.2 Gateway Keepalive Function Configuration

Table 1427 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
	Configure the keepalive function of the IPv6 associated gateway

11.2.2.1 Configure Gateway Keepalive Function

Configuration Condition

Before configuring the gateway keepalive function, first complete the following task:

- Configure the IP address of the interface

Configure Gateway Keepalive Basic Function

Table 1428 Configure the gateway keepalive basic function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Configure the gateway keepalive	keepalive gateway *ip-address* [*interval* | msec *interval*] [*retry-count*] [*delay-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 1429 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.

Configure the Keepalive Function of IPv6 Associated Gateway

After the keepalive function of the IPv6 associated gateway is configured, the interface IPv6 protocol layer will be closed at the same time when the gateway is not reachable.

Table 1430 Configure the keepalive function of the IPv6 associated gateway

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the sending rate of the keepalive packets	keepalive gateway ipv6-respond-ipv4	Optional By default, the keepalive function of the IPv6 associated gateway is disabled.

11.2.2.2 Monitoring and Maintaining of Gateway Keepalive

Table 1431 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
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

11.2.3 Typical Configuration Example of Gateway Keepalive

11.2.3.1 Configure Gateway Keepalive

Network Requirements

- Device4 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

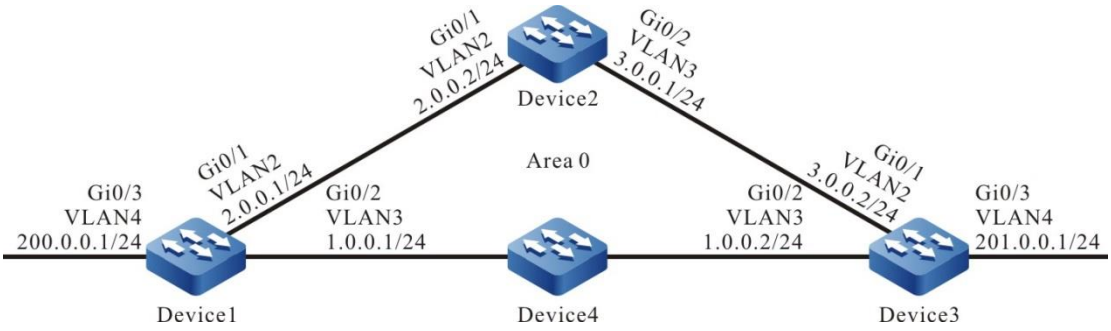


Figure 317 Networking of configuring the gateway keepalive

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 delay 1 remain 0 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 delay 1 remain 0 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 delay 1 remain 1 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.

11.3 SLA

11.3.1 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.

- LSP-ping entity: Used to detect the MPLS network communication
- 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.

11.3.2 SLA Function Configuration

Table 1432 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 ICMPv6-echo entity
	Configure the ICMP-path-echo entity
	Configure the ICMP-path-jitter entity
	Configure the VoIP-jitter entity
	Configure the UDP-echo 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

Configuration Task	
Configure pausing scheduling the entity	Configure pausing scheduling the entity
Configure restoring scheduling the entity	Configure restoring scheduling the entity

11.3.2.1 Enable RTR

In the configuration tasks of RTR, first enable RTR so that the configuration of the other functions can take effect.

Configuration Condition

None

Enable RTR

Table 1433 Enable RTR

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable RTR	rtr enable	Mandatory By default, do not enable RTR.

11.3.2.2 Configure RTR Entity

Configuration Condition

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 1434 Create the RTR entity

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
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 1435 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
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 RTT value as the judgment basis to detect whether the entity is reachable	status-care rtt	Optional By default, RTT value is not used to determine whether it is reachable.
Configure the egress	out-interface interfacename	Optional

Step	Command	Description
interface of the entity		By default, the out interface of the entity is not configured, and the out interface is selected by the routing module When the destination has multiple paths, you can configure the out interface to select one path.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note

- The scheduling interval (frequency-value) 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 ICMPV6-echo Entity

The function of ICMPv6 echo entity is to detect the basic network communication. It regularly sends ICMP echo request packet to a destination address in the network, so as to get the delay and packet loss of packet transmission from detection end to destination. In a detection cycle, as long as an ICMP echo request response packet is received by an ICMP V6 echo entity, the status of the entity is reachable.

Because the general network devices support ping, this entity can play a role in

detecting the basic communication of the network. Through abundant scheduling polities and logging functions, network administrators can know the network communication situation and historical information in time, and reduce the tedious input of the common ping command.

Table 1436 Configure the ICMPV6-echo entity

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the ICMP-echo entity configuration mode	rtr entity-id [icmpv6echo]	-
Configure the detection attributes	set [vrf vrf-name] target-ip-address [npacket] [data-size] [timeout] [frequency-value] [extend source-ip-address [tos] [verify-data]]	Mandatory By default, do not configure the detection attribute of the entity.
Configure RTT value as the judgment basis to detect whether the entity is reachable	status-care rtt	Optional By default, RTT value is not used to determine whether it is reachable.
Configure the common configuration of the entity	Refer to “Configure Common Configuration of the Entity”	Optional

Note

- The scheduling interval (frequency-value) of the ICMPv6-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 1437 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
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.

Step	Command	Description
		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 1438 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

Step	Command	Description
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 1439 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	threshold-sd-delay *sd-delay* direction { be | se }	Optional By default, the sd delay threshold is 5000ms and the over-limit rule is be.

Step	Command	Description
rule		
Configure the uni-directional jitter threshold from the source to the destination and over-limit rule	threshold-sd-jitter *sd-jitter* direction { be | se }	Optional 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 1440 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* [udpecho]	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 By default, do not configure the detection attribute.
Configure the filling content of the packet	data-pattern *pad*	Optional By default, the filling content is "ABCD".
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 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 1441 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.

Step	Command	Description
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 1442 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.
Configure the period of saving the history records	periods *periods*	Optional By default, after each scheduling ends, save one history record.
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

Step	Command	Description
		ICMPv6-echo entity FLOW-statistics entity
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 ICMPv6-echo 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 ICMPv6-echo entity FLOW-statistics 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 ICMPv6-echo entity VoIP-jitter entity FLOW-statistics 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 ICMP-path-jitter entity 70 bytes

Step	Command	Description
		UDP-echo entity 16 bytes The entities not supporting the command: ICMP-echo entity ICMPv6-echo entity VoIP-jitter entity FLOW-statistics 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 ICMPv6-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
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 ICMPv6-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. The entities not supporting the command: FLOW-statistics 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.

11.3.2.3 Configure RTR Entity Group

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 Condition

Before configuring the RTR entity group, first complete the following task:

- Enable RTR.

Configure RTR Entity Group

Table 1443 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 *interval*	Optional

Step	Command	Description
interval between the members in the RTR entity group		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.

11.3.2.4 Configure RTR Responder

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 Condition

Before configuring the RTR responder, first complete the following task:

- Enable RTR.

Configure RTR Responder

Table 1444 Configure the RTR responder

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the RTR responder	rtr responder	Mandatory By default, do not configure the RTR responder.

11.3.2.5 Configure RTR Scheduler

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 Condition

Before configuring the RTR scheduler, first complete the following task:

- Configure the desired RTR entity or RTR entity group

Configure RTR Scheduler

Table 1445 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*	Mandatory By default, do not configure the RTR

Step	Command	Description
	life { forever | *life-time* repeat *repeat-times* }	scheduler.

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.

11.3.2.6 Configure Pausing Scheduling Entity

For the entity being scheduled, we can configure pausing scheduling the entity.

Configuration Condition

Before configuring pausing scheduling the entity, first complete the following task:

- The entity is being scheduled

Configure Pausing Scheduling Entity

Table 1446 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 By default, do not pause the entity in the scheduling state.

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.

11.3.2.7 Configure Restoring Scheduling Entity

For the entity paused scheduling, we can configure restoring scheduling the entity.

Configuration Condition

Before configuring restoring scheduling the entity, first complete the following task:

- The entity is in the paused scheduling state

Configure Restoring Scheduling Entity

Table 1447 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

11.3.2.8 SLA Monitoring and Maintaining

Table 1448 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

11.3.3 SLA Typical Configuration Example

11.3.3.1 Configure ICMP-echo Entity to Detect Basic Network Communication

Network Requirement

- Use the ICMP-echo entity on Device1, detecting the basic communication of the network from Device1 to Device3.

Network Topology

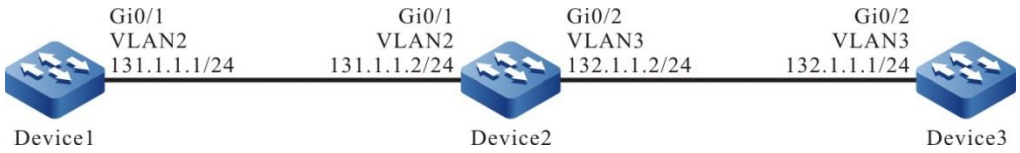


Figure 318 Networking of configuring ICMP-echo entity

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:FALSE Description entity is not scheduled.

Status:DEFAULT Description 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.

11.3.3.2 Configure ICMP-path-echo Entity to Detect Network Communication

Network Requirement

- Use the ICMP-path-echo entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

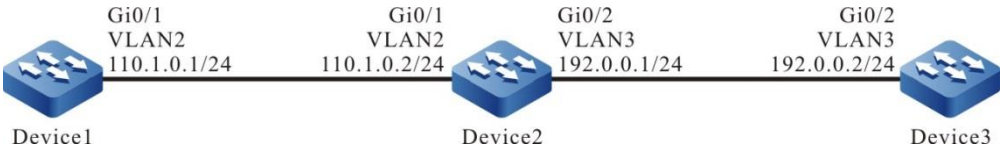


Figure 319 Networking of configuring the ICMP-path-echo entity

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.

```
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.

11.3.3.3 Configure ICMP-path-jitter Entity to Detect Network Communication

Network Requirement

- Use the ICMP-path-jitter entity on Device1, detecting the path network communication from Device1 to Device3.

Network Topology

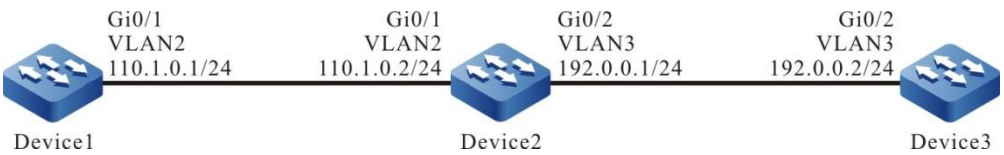


Figure 320 Networking of configuring the ICMP-path-jitter entity

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.

11.3.3.4 Configure VoIP-jitter Entity to Detect Network Transmitting VoIP Packets

Network Requirement

- Use the VoIP-jitter entity on Device1 and detect the network transmitting VoIP packets from Device1 to Device3.

Network Topology

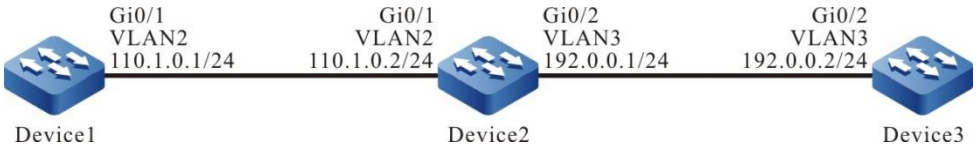


Figure 321 Networking of configuring the VoIP-jitter entity

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.

11.3.3.5 Configure UDP-echo Entity to Detect Network Transmitting UDP Packets

Network Requirement

- Use the UDP-echo entity on Device1 and detect the network transmitting UDP packets from Device1 to Device3.

Network Topology

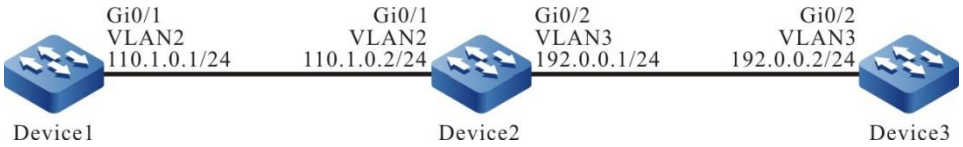


Figure 322 Networking of configuring the UDP-echo entity

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.

11.3.3.6 Configure FLOW-statistics Entity to Detect Interface Traffic

Network Requirement

- Use the FLOW-statistics entity on Device1 and detect the flow of the interface vlan2.

Network Topology

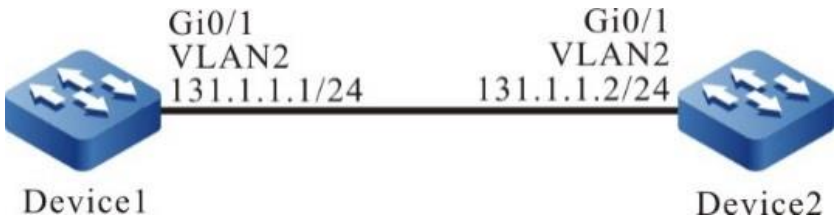


Figure 323 Networking of configuring the FLOW-statistics entity

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: On Device1, configure the FLOW-statistics entity, and add the attribute 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 the 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 result shows that the entity parameter is consistent with the configuration.

Status:DEFAULT indicates that the entity status is DEFAULT.

Step 3: Schedule the defined flow statistics 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 4: Check the result.

When there is the data flow received on interface vlan2:

#View the 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, that is, there are packets entering/leaving interface vlan2.

When there is no flow entering/leaving interface vlan2:

#View the 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 no flow enters/leaves interface vlan2, and the entity status is unreachable.

#View the history record content.

```
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 rate (quantity-based and bit-based) of entering/leaving interface vlan2 during each scheduling is recorded in details in the history records.

Note

- The accessibility of the FLOW-statistics entity is defined as: when the entity is in scheduling, as long as there is traffic in or out direction of the interface, the entity status is reachable, and if there is no traffic, it is unreachable.

11.3.3.7 Configure ICMP-echo ipv6 Entity to Detect Network Communication

Network Requirement

- Use the ICMP echo ipv6 entity on Device1 to detect the basic network communication between Device1 and Device3.

Network Topology

Figure 7 Networking of configuring the ICMP-echo ipv6 entity

Configuration Steps

Step 1: Configure the IPv6 address, route of the interface, so that Device1 and Device3 can communicate with each other. (omitted)

Step 2: Configure the ICMP-echo ipv6 entity, and add the attribute parameters.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
Device1(config-rtr-icmpv6echo)#set 2136::2 5 70 2 12 extend 2135::1 0 TRUE
Device1(config-rtr-icmpv6echo)#alarm-type log
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpv6echo)#threshold-rtt 1000  direction be
Device1(config-rtr-icmpv6echo)#exit
```

#View the ICMP-echo ipv6 entity parameters.

```
Device1#show rtr entity 1
-----------------------------------------------------------------
ID:1          name:Icmpv6Echo1          Created:TRUE
****************type:ICMPV6ECHO****************
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:0
TargetIpv6:2136::2
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:
sourceIpv6:2135::1     tos:0   Verify-data:TRUE
In-scheduling:FALSE
Schedule frequency:12(s)
Status:DEFAULT
------------------------------------------------------------
```

The result shows that the entity parameters are consistent with the configuration.

In-scheduling:FALSE indicates that the entity does not schedule.

Status:DEFAULT indicates that the 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 not reachable, the status is UNREACHABLE.

Step 3: Schedule the defined ICMP-echo ipv6 entity, and define the attribute parameters of the scheduling.

#Configure Device1.

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 20 life forever
```

Step 4: Check the result.

When the network connectivity between Device1 and Device3 is normal:

#View the entity status.

```
Device1#show rtr entity 1
------------------------------------------------------------
ID:1          name:Icmpv6Echo1          Created:TRUE
****************type:ICMPV6ECHO****************
CreatedTime:Tue Sep 17 10:05:52 2019
```

```
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:2
Time-of-last-schedule:Tue Sep 17 10:24:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:10
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:
sourceIpv6:2135::1     tos:0   Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:REACHABLE
------------------------------------------------------------
```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status:REACHABLE indicates that the entity status is reachable, that is, the network connectivity between Device1 and Device3 is normal.

When the network connectivity between Device1 and Device3 fails:

Because the entity parameters are configured with the alarm mode of log, when reaching or exceeding the threshold value, print the alarm information as follows:

```
%SLA-4:Rtr 1 (ICMPV6ECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#View the entity status.

```
Device1#show rtr entity 1
------------------------------------------------------------
ID:1          name:Icmpv6Echo1             Created:TRUE
****************type:ICMPV6ECHO****************
CreatedTime:Tue Sep 17 10:05:52 2019
LatestModifiedTime:Tue Sep 17 10:21:06 2019
Times-of-schedule:21
Time-of-last-schedule:Tue Sep 17 10:28:08 2019
TargetIpv6:2136::2
Transmit-packets:5
Totally-send-packets:105
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:
sourceIpv6:2135::1     tos:0    Verify-data:TRUE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
----------------------------------------------------------------
```

In-scheduling:TRUE indicates that the entity is in scheduling.

Status:UNREACHABLE indicates that the entity status is unreachable, that is, the network connectivity between Device1 and Device3 is unreachable.

#View the history record content.

```
Device1#show rtr history 1
----------------------------------------------------------------
ID:1    Name:Icmpv6Echo1       CurHistorySize:4       MaxHistorysize:255
History recorded as following:
Tue Sep 17 10:24:42 2019
       PktLoss:5        ,Rtt:invalid
Tue Sep 17 10:24:29 2019
       PktLoss:1        ,Rtt:400       (ms)
Tue Sep 17 10:24:17 2019
       PktLoss:0        ,Rtt:1         (ms)
Tue Sep 17 10:24:05 2019
       PktLoss:0        ,Rtt:0         (ms)
----------------------------------------------------------------
```

The packet loss and delay of each scheduling are recorded in detail in the history record; RTT is invalid, which indicates that the network is not reachable due to the failure in the network.

11.3.3.8 Configure TRACK to Link with SLA

Network Requirement

- TRACK links with SLA. Judge the validity of the static route on Device1 via the entity status.

Network Topology

Figure 324 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.

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, vlan2
```

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.

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.

11.3.3.9 Configure TRACK to Link with ICMP-echo ipv6

Network Requirement

- TRACK links with SLA. Judge the validity of the static route on Device1 via the entity status.

Network Topology

Figure 325 Networking of configuring TRACK to link with icmp-echo ipv6

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: On Device1, configure the ICMP-echo ipv6 entity to detect the network connectivity between Device1 and Device2, and add the entity to the entity group.

#Configure Device1.

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpv6echo
```

```
Device1(config-rtr-icmpv6echo)# set 2135::2 5 70 2 12 extend 2135::1 0 FALSE
Device1(config-rtr-icmpv6echo)#number-of-history-kept 255
Device1(config-rtr-icmpv6echo)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
```

Step 3: Define TRACK, and associate SLA.

#Configure Device1.

```
Device1(config)#track 1
Device1(config-track)#rtr 1
Device1(config-track)#exit
```

Step 4: Add static route and associate TRACK.

#Configure Device1.

```
Device1(config)#ipv6 route 2136::/64 2135::2 track 1
```

Step 5: Schedule the entity group.

#Configure Device1.

```
Device1(config)#rtr schedule 1 group 1 start now ageout 20 life forever
```

Step 6: Check the result.

When the network connectivity between Device1 and 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 REACHABLE.

#In the route table of Device1, view the route of network segment 2136::/64.

```
Device1#show ipv6 route 2136::/64
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
```

```
S   2136::/64 [1/0]
    via 2135::2 [0], 00:50:17, vlan100
        2135::2 [0], vlan100
```

The result shows that there is the route to the segment 2136::/64, indicating that when the status of the entity group is REACHABLE, judge that the associated static route is valid.

When the network connectivity between Device1 and Device2 fails:

#View the entity group status.

```
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 network segment 2136::/64.

```
Device1#show ipv6 route 2136::/64
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
```

The result shows that there is no route to the segment 2136::/64, indicating that when the status of the entity group is UNREACHABLE, judge that the associated static route is invalid.

11.4 NTP

11.4.1 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.

In the actual application, select the appropriate NTP work mode according to the network deployment, so as to meet the network clock synchronization requirement in different environments. NTP supports the following three work modes:

Client/server mode

In the client/server mode, the client sends the clock synchronization packet with Mode field 3 (client mode) to the server. After receiving the packet, the server automatically works in the server mode and sends the response packet with Mode field 4 (server mode). After receiving the response packet, the client synchronizes the system clock. In the mode, the client can synchronize the clock from the server, while the server cannot synchronize the clock from the client.

- Peer mode

In the peer mode, the active peer and passive peer first interact the NTP packet with the Mode field 3 (client mode) and 4 (server mode). And then, the active peer sends the clock synchronization packet with the M ode field 1 (the active peer mode) to the passive peer. After receiving the packet, the passive peer automatically works in the passive peer mode and sends the clock synchronization packet with the Mode field 2 (passive peer mode). In this way, the peer mode is set up. In the mode, the active peer and the passive peer synchronize the clock mutually. If the clocks of the two parties are already synchronized, be subject to the clock with smaller layers.

- Broadcast mode

In the broadcast mode, the broadcast server periodically sends the clock synchronization packet with the Mode field 5 (broadcast server mode) to the broadcast

address 255.255.255.255, and the broadcast client monitors the broadcast packet from the broadcast server. When the broadcast client receives the first broadcast packet, the broadcast client and broadcast server interact the NTP packet with the Mode field 3 (client mode) and 4 (server mode), so as to get the network delay of the broadcast client and broadcast server. And then, the broadcast client continues to monitor the broadcast packet and synchronizes the system clock according to the received broadcast packet.

11.4.2 NTP Function Configuration

Table 1449 NTP function configuration list

Configuration Task	
Configure the NTP basic functions	Configure the NTP client/server mode
	Configure the NTP peer mode
	Configure the NTP broadcast mode
Configure the NTP optional parameters	Configure the NTP reference clock
	Configure the source interface of the NTP packet
	Configure the receiving and sending control of the NTP packet
	Configure the quantity of the NTP dynamic sessions
Configure the NTP authentication functions	Configure the NTP client/server authentication
	Configure the NTP peer authentication
	Configure the NTP broadcast authentication
Configure the NTP access control	Configure the NTP access control

11.4.2.1 Configure NTP Basic Functions

Configuration Condition

Before configuring the NTP basic functions, first complete the following task:

- Configure the network layer address of the interface, making the network layer between the NTP clock service requester and clock service provider reachable.
- The NTP clock service provider enables NTP.

Configure NTP Client/Server Mode

When using the NTP client/server mode, do not need special configuration on the server, but it is necessary to ensure that the serve clock is synchronized and the clock layers of the server are smaller than the clock layers of the client.

Perform the following configuration on the NTP client.

Table 1450 Configure the NTP client

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Specify the NTP server	ntp server [vrf *vrf-name*] { *ip-address* | ipv6 *ipv6-address* | *domain-name* } [version *version-number* | key *key-number* | source *interface-name*]*	Mandatory By default, do not specify the NTP server.

Note

- The *ip-address* parameter is one unicast address, but cannot be the broadcast address, multicast address or IP address of the local device.
- The *ipv6-address* parameter is one global unicast address or Link-Local address, but cannot be the multicast address.
- After specifying the source interface of the client packet via **source** *interface-name*, the master IP address of the interface or the first global unicast IPv6 address is set as the source IP address of the packet sent by the client. If the configured server address is IPv6 Link-local address, you should specify the source interface.
- You can specify multiple servers by configuring the **ntp server** or **ntp server ipv6** command for multiples times. You can specify 64 servers at most (the total of ipv4+ipv6+domain names).

Configure NTP Peer Mode

When using the NTP peer mode, do not need special configuration on the passive peer, but it is necessary to ensure that the passive peer can receive and send the NTP packet. You can enable NTP by configuring the **ntp enable (ipv6)** command on the passive peer or any NTP command in "1.2.1 Configure NTP Basic Functions".

Perform the following configuration on the NTP active peer.

Table 1451 Configure the NTP active peer

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Specify the NTP passive peer	ntp peer [vrf *vrf-name*] { *ip-address* | ipv6 *ipv6-address* | *domain-name* } [version *version-number* | key *key-number* | source *interface-name*] *	Mandatory By default, do not specify the NTP passive peer.

Note

- The *ip-address* parameter is one unicast address, but cannot be the broadcast address, multicast address or IP address of the local device.
- The *ipv6-address* parameter is one global unicast address or Link-Local address, but cannot be the multicast address.
- After specifying the sending source interface of the active peer packet via **source** *interface-name*, the master IP address of the interface or first global unicast IPv6 address is set as the source IP address of the packet sent by the active peer. If the configured peer address is the IPv6 Link-local address, you should specify the source interface.
- You can specify multiple passive peers by configuring the **ntp server** or **ntp peer ipv6** command for multiples times. You can specify 64 passive peers at most (the total of IPv4+IPv6 +domain name).

Configure NTP Broadcast Mode

When using the NTP broadcast mode, the broadcast server and broadcast client both need to be configured and it is necessary to ensure that the clock of the broadcast server is synchronized and the clock layers are smaller than the clock layers of the broadcast client. It is necessary to specify one interface for sending the NTP broadcast packet on the broadcast server and one interface for receiving the NTP broadcast packet on the broadcast client, so the configuration of the broadcast mode can only be performed in the specific interface mode.

Perform the following configuration on the NTP broadcast client.

Table 1452 Configure the NTP broadcast client

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the NTP broadcast client on the interface	ntp broadcast client	Mandatory By default, the interface does not enable the NTP broadcast client.

Perform the following configuration on the NTP broadcast server.

Table 1453 Configure the NTP broadcast server

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the interface configuration mode	interface *interface-name*	-
Enable the NTP broadcast server on the interface	ntp broadcast-server [key *key-number* | version *version-number*]*	Mandatory By default, the interface does not enable the NTP broadcast server.

11.4.2.2 Configure NTP Optional Parameters

Configuration Condition

None

Clock NTP Reference Clock

NTP can synchronize the system time via the following two modes:

- Synchronize with the local clock, that is, adopt the local clock as the NTP reference clock
- Synchronize with the other clock source in network, that is, use any of the previous mentioned three NTP work modes.

Table 1454 Configure the local clock as the NTP reference clock

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the local clock as the NTP reference clock	ntp master [*stratum-number*]	Mandatory By default, do not configure the local clock as the NTP reference clock.

Note

- After configuring the local clock as the NTP reference clock, NTP cannot synchronize the clock from the other clock source in the network.
- After configuring the local clock as the NTP reference clock, the local device can serve as the clock source to synchronize the other device in the network. Please use the configuration carefully, so as to avoid the clock error of other device in the network.

Configure Source Interface of the NTP Packet

If the source interface of the NTP packet is configured and when the device actively sends the NTP packet, select the master IP address of the specified source interface as the source IP address of the packet.

Table 1455 Configure the source interface of the NTP packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the source interface of the NTP packet	ntp source *interface-name*	Mandatory By default, do not configure the source interface of the NTP packet.

Note

- If using the **ntp server** or **ntp peer** command to specify the source interface, first use the source interface specified by the **ntp server** or **ntp peer** command.
- If **ntp broadcast i**s configured in the interface mode, the source interface of the NTP broadcast packet is the interface configured with the above command.
- If the source interface of the specified NTP packet is down, restore the master address of the default routing interface or the first global unicast address to encapsulate the source address of NTP.
- If the source interface of the specified NTP packet is not configured with address and is in the up state, but there is no corresponding IPv4 or IPv6 address, restore the master address of the default routing interface or the first global unicast address to encapsulate the source address of NTP.

Configure Receiving and Sending Control of NTP Packet

By default, the device will not receive and send all NTP packets. You can configure the receiving and sending control of the NTP packet to enable receiving and sending the NTP packet.

Table 1456 Configure the receiving and sending control of the NTP packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable receiving and sending the NTP packet	ntp enable [ipv6]	Mandatory By default, do not prohibit receiving and sending the NTP packet.

Note

- After configuring the command **no ntp enable**, it will be forbidden to receive and send all the NTP packets of IPv4. If configuring the command **ntp enable**, it will enable receiving and sending the NTP packets of IPv4.
- After configuring the command **no ntp enable ipv6**, it will be forbidden to receive and send all IPv6 NTP packets. If configuring the command **ntp enable ipv6**, it will enable receiving and sending IPv6 NTP packets.

Configure the Number of NTP Dynamic Sessions

Set the maximum number of NTP dynamic connections allowed locally by configuring the number of NTP dynamic sessions.

Table 1457 Configure the number of the NTP dynamic sessions

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Set the maximum number of NTP dynamic connections allowed locally	ntp max-dynamic-sessions *number*	Mandatory By default, the number of the dynamic NTP sessions allowed to be

Step	Command	Description
		set up is 100.

11.4.2.3 Configure NTP Authentication Function

In the network with high requirement for the security, when running the NTP protocol, it is necessary to enable the authentication function. Authenticate the packet interacted by the NTP clock service requester and clock service provider to ensure that the clock service requester is synchronized with the valid time, improving the network security.

Configuration Condition

To configure the NTP authentication function, first complete the following task:

- Configure the network layer address of the interface, making the network layer between the NTP clock service requester and clock service provider reachable.
- The NTP clock service provider enables NTP.

Configure NTP Client/Server Authentication

When configuring the NTP client/server authentication, it is necessary to enable the authentication function on the client and server, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the server on the client.

Perform the following configuration on the NTP client.

Table 1458 Configure the NTP client authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not

Step	Command	Description
		enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Configure the specified key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do not specify the trusted key.
Specify the key associated with the server	ntp server [vrf *vrf-name*] { *ip-address* | *domain-name* | ipv6 *ipv6-address* } [version *version* | source *interface-name*] key *key-number*	Mandatory

Perform the following configuration on the NTP server.

Table 1459 Configure the NTP server authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do not

Step	Command	Description
		specify the trusted key.

Note

- The server and client need to be configured with the same authentication key.

Configure NTP Peer Authentication

When configuring the NTP peer authentication, it is necessary to enable the authentication function on the active peer and passive peer, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the passive peer on the active peer.

Perform the following configuration on the NTP active peer.

Table 1460 Configure the NTP active peer authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do

Step	Command	Description
		not specify the trusted key.
Specify the key associated with the passive peer	ntp peer [vrf *vrf-name*] *ip-address* | *domain-name* | ipv6 *ipv6-address* [version *version* | source *interface-name*] key *key-number*	Mandatory

Perform the following configuration on the NTP passive peer.

Table 1461 Configure the NTP passive peer authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do not specify the trusted key

Note

- The active peer and passive peer need to be configured with the same authentication key.

Configure NTP Broadcast Authentication

When configuring the NTP broadcast authentication, it is necessary to enable the authentication function on the broadcast client and broadcast server, configure the authentication key, set the authentication key as the trusted key, and specify the key associated with the broadcast server.

Perform the following configuration on the NTP broadcast client.

Table 1462 Configure the NTP broadcast client authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do not specify the trusted key.

Perform the following configuration on the NTP broadcast server.

Table 1463 Configure the NTP broadcast server authentication

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the NTP authentication function	ntp authenticate	Mandatory By default, do not enable the NTP authentication function.
Configure the authentication key	ntp authentication-key *key-number* md5 {0 *plain-key* | 7 *cipher-key*}	Mandatory By default, do not configure the authentication key.
Specify the key as the trusted key	ntp trusted-key *key-number*	Mandatory By default, do not specify the trusted key.
Enter the interface configuration mode	interface *interface-name*	-

Step	Command	Description
Specify the key associated with the broadcast server	ntp broadcast-server [version *version-number*] key *key-number*	Mandatory

Note

- The broadcast server and broadcast client need to be configured with the same authentication key.

11.4.2.4 Configure NTP Access Control

Configuration Condition

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 1464 Configure the NTP access control

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the NTP access control	ntp access-control list *access-list-name*	Mandatory By default, do not configure the NTP access control.

11.4.2.5 NTP Monitoring and Maintaining

Table 1465 NTP Monitoring and Maintaining

Command	Description
show ntp associations [ipv6]	Display the NTP session information
show ntp status	Display the NTP status information

Command	Description
snmp-server enable traps ntp [stratum-change | sync-lost | sync-success]*	Enable the Trap function of NTP

11.4.3 NTP Typical Configuration Example

11.4.3.1 Configure NTP IPv4 Server/Client Mode

Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.
- Device1 and Device2 are interconnected via their interfaces VLAN2 and the route is reachable.
- The NTP server is the clock source and the client gets the clock from the server.

Network Topology

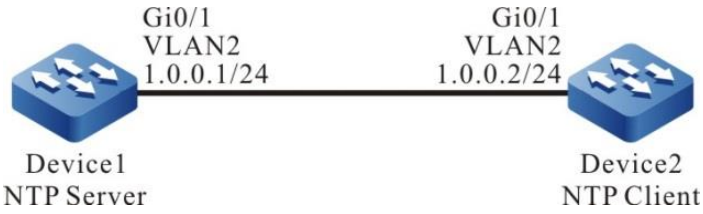


Figure 326 Networking of configuring NTP server and client

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 of device1, configure the time zone as Beijing time zone, local clock as reference clock, and the number of clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

```
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable NTP IPv4 of device2, and configure the time zone as Beijing time zone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 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 4: 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
 NTP ipv4 is enabled
 NTP ipv6 is disabled
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
```

Configure NTP IPv4 Server/Multi-level Client Mode

Network Requirement

- Device1 is the NTP server; Device2 and Device3 are the NTP clients.
- Device2 are interconnected with Device1 and Device 3 via interface vlan2, vlan3; the route is reachable.
- Device1 provides the clock for Device2; Device2 provides the clock for

Device3.

Network Topology

Figure 327 Networking of configuring the NTP server and multi-level clients

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 of device1, configure the time zone as Beijing time zone, local clock as reference clock, and the number of clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit Device1(config)#ntp master 3
```

Step 3: Configure the NTP client Device2.

#Enable the NTP IPv4 function of Device2, and configure the time zone as Beijing time zone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Step 4: Configure the NTP client Device3.

#Enable the NTP IPv4 function of Device3, and configure the time zone as Beijing time zone.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BINJING 8
```

#Specify the NTP server Device2 and the IP address is 2.0.0.1.

```
Device2(config)#ntp server 2.0.0.1
```

Step 5: 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
NTP ipv4 is enabled
NTP ipv6 is disabled
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
NTP ipv4 is enabled
NTP ipv6 is disabled
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
```

11.4.3.2 Configure NTP IPv4 Server/Multi-level Client Mode

Network Requirement

- Device1 is the NTP server; Device2 and Device3 are the NTP clients.
- Device2 are interconnected with Device1 and Device 3 via interface vlan2, vlan3; the route is reachable.
- Device1 provides the clock for Device2; Device2 provides the clock for Device3.

Network Topology

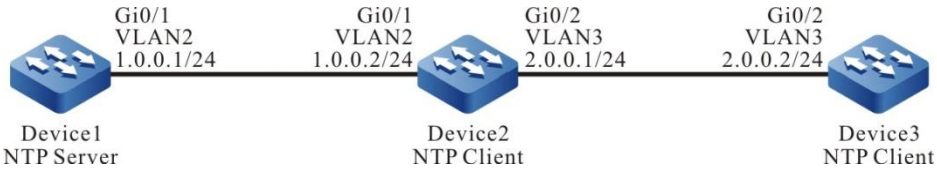


Figure 328 Networking of configuring the NTP server and multi-level clients

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv4 of device1, configure the time zone as Beijing time zone, local clock as reference clock, and the number of clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit Device1(config)#ntp master 3
```

Step 3: Configure the NTP client Device2.

#Enable the NTP IPv4 function of Device2, and configure the time zone as Beijing time zone.

```
Device2#configure terminal
```

```
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1 and the IP address is 1.0.0.1.

```
Device2(config)#ntp server 1.0.0.1
```

Step 4: Configure the NTP client Device3.

#Enable the NTP IPv4 function of Device3, and configure the time zone as Beijing time zone.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BINJING 8
```

#Specify the NTP server Device2 and the IP address is 2.0.0.1.

```
Device2(config)#ntp server 2.0.0.1
```

Step 5: 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
NTP ipv4 is enabled
NTP ipv6 is disabled
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
NTP ipv4 is enabled
NTP ipv6 is disabled
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
```

11.4.3.3 Configure the NTP Server and Client with MD5 Authentication

Network Requirement

- Device1 is the NTP server; Device2 is the NTP client, and they adopt the MD5 algorithm authentication.
- Device1 is interconnected with Device2 via their interface vlan2; the route is reachable.
- The NTP server is the clock source, and the client gets the clock from the server.

Network Topology

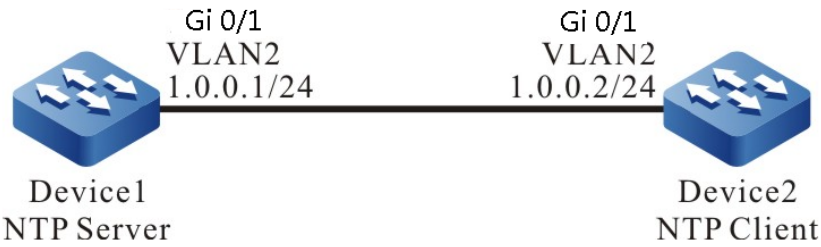


Figure 329 Networking of configuring the NTP server and client with MD5 authentication

Configuration Steps

Step1: Configure the IP address of the interface (omitted).

Step 2: Configure the NTP server.

#Enable NTP IPv4 of Device1, configure the time zone as Beijing time zone, local clock as the reference clock, and the layers of the clock as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

#Enable the authentication.

```
Device1(config)#ntp authenticate
```

#Configure the authentication key No. as 1, algorithm as MD5, and key as admin.

```
Device1(config)#ntp authentication-key 1 md5 0 admin
```

#Configure key 1 to be trusted.

```
Device1(config)#ntp trusted-key 1
```

Step 3: Configure the NTP client.

#Enable NTP IPv4 of Device2, and configure the time zone as Beijing time zone,

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 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
```

#Enable authentication.

```
Device2(config)#ntp authenticate
```

#Configure the authentication key No. as 1, algorithm as MD5, and key as admin.

```
Device2(config)#ntp authentication-key 1 md5 0 admin
```

#Configure key 1 to be trusted.

```
Device2(config)#ntp trusted-key 1
```

Step 4: Check the result.

#Execute the **show ntp status** command on the client Device2 to view the clock synchronization status and other information, indicating that the client and the NTP server device1 have been synchronized, and the number of clock layers is 4, larger than that of Device1 by 1.

```
Device2#show ntp status
Current NTP status information
 NTP ipv4 is enabled
NTP ipv6 is disabled
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442ECE1.8BB7B219 (01:56:49.545 Tue Nov 06 2012)
```

#On Device2, execute the **show clock** command to view the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:56:52 2012
```

Caution

- The authentication serial number of NTP client and server must be the same, and the key must be the same.

11.4.3.4 Configure NTP IPv4 Peer Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device2 is the NTP client; set Device1 to the NTP server.
- Device3 sets Device2 as the peer, Device3 is the active peer, and Device2 is the passive peer.

Network Topology

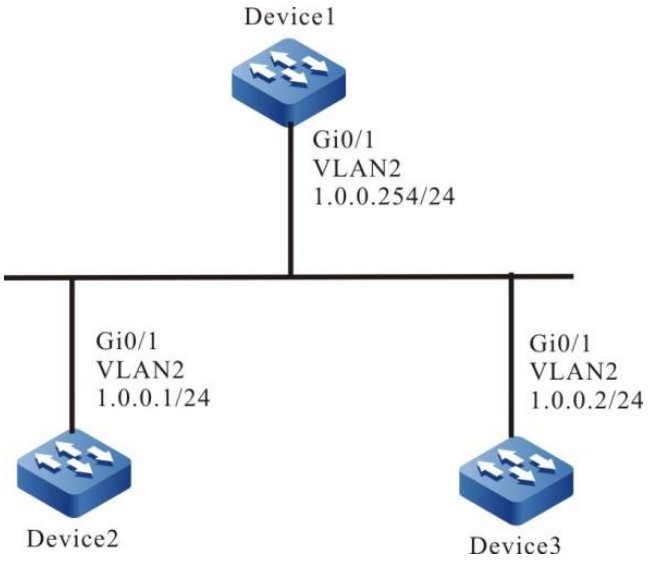


Figure 330 Networking of configuring the NTP peer mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: On Device1, enable NTP IPv4, and configure the time zone as Beijing time zone, and the number of the local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

Step 3: Device2 specifies Device1 as the NTP server.

#On Devie2, enable NTP IPv4, and configure the time zone as Beijing Timezone.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BEIJING 8
```

#Specify the IP address of the NTP server as 1.0.0.254.

```
Device2(config)#ntp server 1.0.0.254
```

Step 4: Device3 sets Device2 as the peer.

#On Device3, enable NTP IPv4, and configure the time zone as Beijing time zone.

```
Device3#configure terminal
Device3(config)#ntp enable
```

```
Device3(config)#clock timezone BEIJING 8
```

#Specify the IP address of the NTP peer as 1.0.0.1.

```
Device3(config)#ntp peer 1.0.0.1
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
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 layers of Device2 clock is 4, larger than Device1 by 1, and the reference clock server address is 1.0.0.254, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock

BEIJING(UTC+08:00) TUE APR 28 11:10:36 2015
```

#Execute the **show ntp status** command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
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 layers of Device3 clock is 5, larger than Device2 by 1, and the reference clock server address is 1.0.0.1, indicating that the active peer Device3 is already synchronized with the passive peer Device2.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock
```

BEIJING(UTC+08:00) TUE APR 28 11:16:19 2015

11.4.3.5 Configure NTP Broadcast Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device1 is the NTP broadcast server and sends the NTP broadcast packet from the interface vlan2.
- Device2 and Device3 are the NTP broadcast client, monitoring the NTP broadcast packet on their interface vlan2.

Network Topology

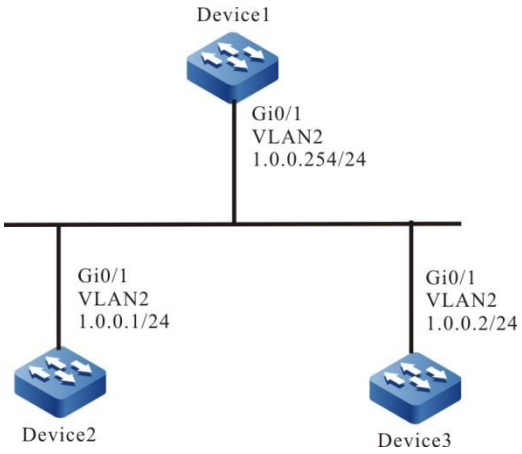


Figure 331 Networking of configuring the NTP broadcast mode

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Device1 sets the local clock as the reference clock and the number of the layers is 3; configure Device1 as the NTP broadcast server, sending the NTP broadcast packet from the interface vlan2.

#On Device1, enable NTP IPv4, and configure the time zone as Beijing time zone, and the number of the local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

#Configure Device1 as the NTP broadcast server, sending the NTP broadcast packet from the interface vlan2.

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ntp broadcast-server
```

Step 3: Configure Device2 as the NTP broadcast client, monitoring the NTP broadcast packet on the interface vlan2.

```
Device2#configure terminal
Device2(config)#ntp enable
Device2(config)#clock timezone BINJING 8
Device2(config)#interface vlan2
Device2(config-if- vlan2)#ntp broadcast-client
```

Step 4: Configure Device3 as the NTP broadcast client, monitoring the NTP broadcast packet on the interface vlan2.

```
Device3#configure terminal
Device3(config)#ntp enable
Device3(config)#clock timezone BINJING 8
Device3(config)#interface vlan2
Device3(config-if- vlan2)#ntp broadcast-client
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
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 Device2 clock layers is 4, larger than Device1 by 1,

and the reference clock server address is 1.0.0.254, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the show clock command to view the device clock on the client Device2.

```
Device2#show clock

BEIJING(UTC+08:00) TUE APR 28 11:27:22 2015
```

#Execute the **show ntp status** command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
NTP ipv4 is enabled
NTP ipv6 is disabled
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 layers of Device3 clock is 4, larger than Device1 by 1, and the reference clock server address is 1.0.0.254, indicating that the active peer Device3 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock

BEIJING(UTC+08:00) TUE APR 28 11:27:41 2015
```

11.4.3.6 Configure NTP IPV6 Server and Client

Network Requirements

- Device1 is the NTP server and Device2 is the NTP client.
- Device1 and Device2 are interconnected via their interfaces VLAN2 and the route is reachable.
- The NTP server is the clock source and the client gets the clock from the server.

Network Topology

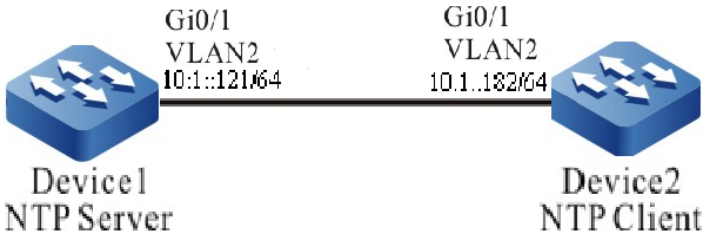


Figure 332 Networking of configuring the NTP IPV6 server and client

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (Omitted)

Step 2: Configure the NTP server Device1.

#Enable NTP IPv6 of device1, configure the time zone as Beijing time zone, local clock as reference clock, and the number of clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
Device1(config)#exit
```

Step 3: Configure the NTP client Device2.

#Enable NTP IPv6 of Device2, and configure the time zone as Beijing time zone.

```
Device2#configure terminal
Device2(config)#ntp enable ipv6
Device2(config)#clock timezone BINJING 8
```

#Specify the NTP server Device1, and IPv6 address as 10:1::121.

```
Device2(config)#ntp server ipv6 10:1::121
Device2(config)#exit
```

Step 4: 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
 NTP ipv4 is disabled
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::121
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#On the client Device2, execute the **show clock** command to view the device clock.

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:49:30 2012
```

11.4.3.7 Configure NTP IPV6 Peer Mode

Network Requirements

- Device1, Device2, and Device3 are interconnected via their interfaces; the route is reachable.
- Device1 sets the local clock as the reference clock and the number of the layers is 3.
- Device2 is the NTP client; set Device1 to the NTP server.
- Device3 sets Device2 as the peer, Device3 is the active peer, and Device2 is the passive peer.

Network Topology

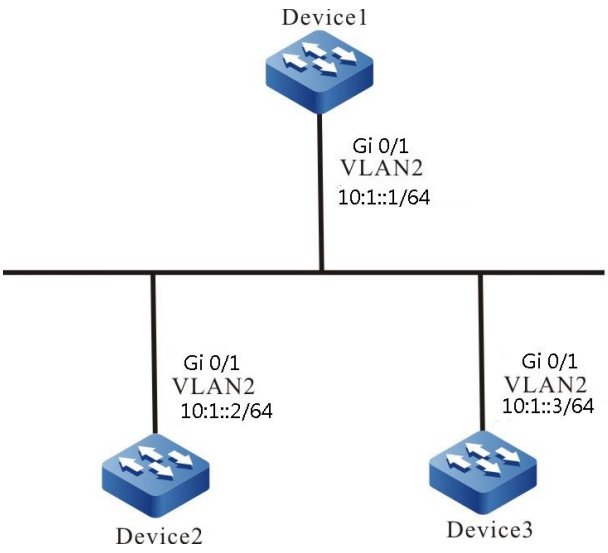


Figure 333 Networking of configuring the NTP IPv6 peer mode

Configuration Steps

Step 1: Configure the IPv6 address of the interface. (omitted)

Step 2: On Device1, enable NTP IPv6, and configure the time zone as Beijing time zone, and the number of the local clock layers as 3.

```
Device1#configure terminal
Device1(config)#ntp enable ipv6
Device1(config)#clock timezone BINJING 8
Device1(config)#ntp master 3
```

Step 3: Device2 specifies Device1 as the NTP server.

#On Devie2, enable NTP IPv6, and configure the time zone as Beijing Time zone.

```
Device2#configure terminal
Device2(config)#ntp enable ipv6
Device2(config)#clock timezone BEIJING 8
```

#Specify the IPv6 address of the NTP server as 10:1::1.

```
Device2(config)#ntp server ipv6 10:1::1
```

Step 4: Device3 sets Device2 as the peer.

#On Device3, enable NTP IPv6, and configure the time zone as Beijing time zone.

```
Device3#configure terminal
Device3(config)#ntp enable ipv6
Device3(config)#clock timezone BEIJING 8
```

#Specify the IPv6 address of the NTP peer as 10:1::2.

```
Device3(config)#ntp peer ipv6 10:1::2
```

Step 5: Check the result.

#Execute the **show ntp status** command on the client Device2 and view the clock synchronization status information.

```
Device2#show ntp status
Current NTP status information
NTP ipv4 is disabled
```

```
NTP ipv6 is enabled
Clock is synchronized, stratum 4, reference is 10:1::1
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

The layers of Device2 clock is 4, larger than Device1 by 1, and the reference clock server address is 10:1::1, indicating that the client Device2 is already synchronized with the server Device1.

#Execute the **show clock** command to view the device clock on the client Device2.

```
Device2#show clock
```

#Execute the show ntp status command on the active peer Device3 and view the clock synchronization status information.

```
Device3#show ntp status
Current NTP status information
 NTP ipv4 is disabled
 NTP ipv6 is enabled
Clock is synchronized, stratum 5, reference is 10:1::2
reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)
```

The layers of Device3 clock is 5, larger than Device2 by 1, and the reference clock server address is 10:1::2, indicating that the active peer Device3 is already synchronized with the passive peer Device2.

#Execute the **show clock** command to view the device clock on client Device3.

```
Device3#show clock
```

11.5 Port Mirror

11.5.1 Overview

11.5.1.1 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, encapsulated remote SPAN, and VLAN SPAN.

11.5.1.2 Basic Concepts

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 or multiple RSPAN VLANs. 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 one RSPAN VLAN. RSPAN destination session sends RSPAN VLAN data to the destination port.

Encapsulated Remote SPAN

Encapsulated remote SPAN, also known as ERSPAN (Encapsulated Remote Switched Port Analyzer), provides the encapsulation of image packets through the specific tunnel, and traverses L3 networks to realize data monitoring. When configuring an ERSPAN session, you need to specify one or more monitoring ports, a source IP address, and a destination IP address.

VLAN SPAN

VLAN SPAN supports the VLAN mirror on one device. Mirror one or multiple monitor VLAN data flow and send to the destination port. The mirrored data flow can be the input data flow and also can be output data flow or mirror the input and output flow at the same time.

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 cannot bear other services any more.

- 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.
- The destination ports of one session can be four at most. According to the chip, different cards may support different numbers of the destination ports.

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.

11.5.2 SPAN Function Configuration

Table 1466 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 source session
Configure VLAN SPAN	Configure the VLAN SPAN session

11.5.2.1 Configure Local SPAN

Local SPAN is used to analyze the data flow of the local device port.

Configuration Condition

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 1467 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* | interface 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- list* | interface 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. The source

of the port mirror session cannot be the same as the source of the flow mirror.

11.5.2.2 Configure RSPAN

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 Condition

None

Configure RSPAN VLAN

RSPAN makes the mirror packet traverse the L2 network by labeling the RSPAN LAN tag on the mirror packet.

Table 1468 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 from the destination port of the RSPAN source session.

Table 1469 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* | interface 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-id* 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.
- RSPAN source session only supports one destination port.

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 1470 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- list* | interface link-aggregation *link-aggregation-id* }	Mandatory By default, do not configure the destination end of the RSPAN destination session.

Note

- 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.

11.5.2.3 Configure VLAN SPAN

The VLAN SPAN session is used to analyze the data flow of the specified VLAN.

Configuration Condition

None

Configure VLAN SPAN Session

VLAN SPAN is similar to Local SPAN. VLAN SPAN session copies the packet received or forwarded by one or multiple source VLANs, and forwards from the destination port. Meanwhile, it does not affect the normal service forwarding of the source VLAN.

Table 1471 Configure the VLAN SPAN session

Step	Command	Description
Enter the global configuration mode	config terminal	-
Configure the source VLAN of the VLAN SPAN session	monitor session *session-number* source vlan [both | tx | rx]	Mandatory By default, do not configure the source VLAN of the VLAN SPAN session.
Configure the destination of the VLAN SPAN session	monitor session *session-number* destination interface *interface- list*	Mandatory By default, do not configure the destination of the VLAN SPAN session.

Note

- The destination port of the VLAN SPAN session cannot be the member port of the VLAN SPAN session source VLAN.
- The destination port of the VLAN SPAN session can only be the general port, but cannot be the aggregation group.
- The member port of the VLAN SPAN session source VLAN cannot be in multiple sessions at the same time.
- When configuring the source VLAN of the VLAN SPAN session and if

the member ports of the source VLAN already belongs to other sessions, these sessions will actively delete these ports.

- The system only supports one VLAN SPAN session.

11.5.2.4 SPAN Monitoring and Maintaining

Table 1472 SPAN Monitoring and Maintaining

Command	Description
show monitor session { session-number | all | local | remote | erspan }	Display the SPAN session configuration information.
show monitor rspan-vlan	Display RSPAN VLAN.

11.5.3 Typical Configuration Example of Port Mirror

11.5.3.1 Configure Local SPAN

Network Requirement

- 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

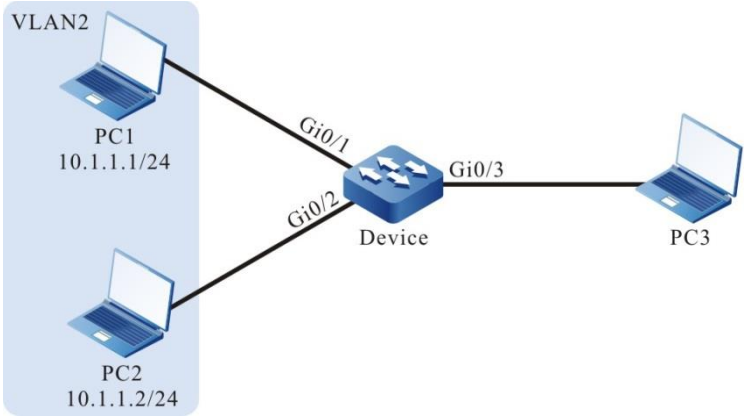


Figure 334 Networking of configuring the Local SPAN

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.

11.5.3.2 Configure RSPAN

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

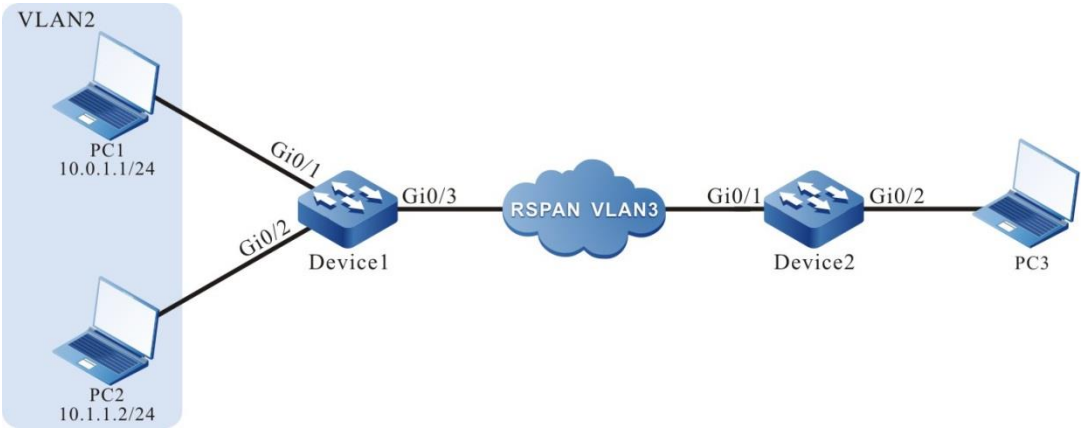


Figure 335 Networking of configuring the RSPAN

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.

11.5.3.3 Configure VLAN SPAN

Network Requirements

- PC1, PC2, and PC3 are connected with Device; PC1 and PC2 communicate in VLAN2.
- Configure VLAN SPAN on Device, the source vlan is vlan2, and the destination port is gigabitethernet0/3, realizing that PC3 monitors the packets received and sent by VLAN2 of Device.

Network Topology

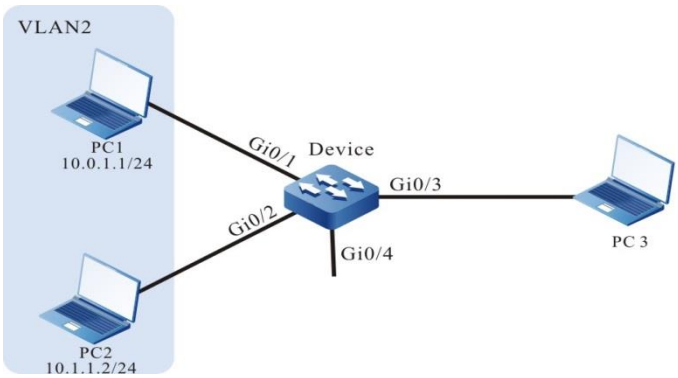


Figure 336 Networking of configuring VLAN SPAN

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
```

#On Device, configure the link type of port gigabitethernet0/1 and 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 VLAN SPAN.

#Configure VLAN SPAN on Device, the mirror source session is vlan2, and the destination session is port gigabitethernet0/3.

```
Device(config)#monitor session 1 source vlan 2 both
Device(config)#monitor session 1 destination interface gigabitethernet0/3
Device#show monitor session all
------------------------------------------------------------
Session 1
Type          : SPAN Local VLAN Session
Destination Interface  : gi0/3
Source VLAN(both): 2
```

Step 3: Check the result.

#When PC1 and PC2 communicate with each other, you can capture the packets received and sent by VLAN2 on PC3.

11.6 sFlow

11.6.1 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.

11.6.2 sFlow Function Configuration

Table 1473 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

11.6.2.1 Configure sFlow Basic Functions

Configuration Condition

None

Create agent Role

The agent role is used to configure and manage the sampling. Currently, the network address type supported by the agent role can only be IPv4.

Table 1474 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 1475 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*] [udp-port *udp-port-number*]	Mandatory By default, do not create the receiver role.

11.6.2.2 Configure sFlow Sampling Mode

Configuration Condition

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 interface flow sampling, the switching chip samples the traffic received by the interface 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 1476 Configure the interface 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 interface regular polling sampling, is to regularly encapsulate the packet and traffic statistics information on the interface within the period and send to the corresponding third-party receiver of the receiver role.

Table 1477 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.

11.6.2.3 sFlow Monitoring and Maintaining

Table 1478 sFlow monitoring and maintaining

Command	Description
clear sflow receiver	Clear the sFlow sampling statistics information

Command	Description
receiver-index statistics	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 interface
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 interface

11.6.3 sFlow Typical Configuration Example

11.6.3.1 Configure sFlow Basic Functions

Network Requirements

- Device is the sFlow agent device and the route with the NMS server is reachable.
- The NMS server monitors the interface data traffic of Device via sFlow.

Network Topology

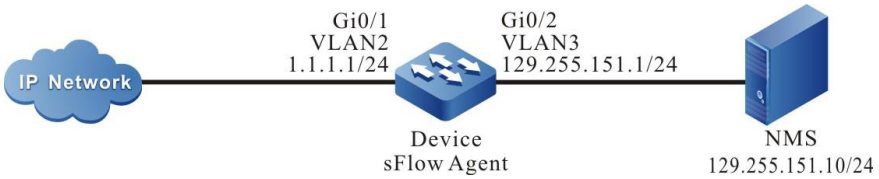


Figure 337 Networking of configuring the sFlow basic functions

Configuration Steps

Step 1: Configure VLAN and add the interface 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 interface 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 interface 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 interface 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    1/10       1/864      1/864      0x00000ab2/0x002a644c
```

```
sFlow Receivers Configuration: (Reset Delta = 18000, Current Tick = 0x002a6476)

sFlow Receivers num:1(limit 10)

                                                                  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:

sFlow Samplers num:1(limit 864)


 Sampling Types: H - raw packet header  E - ethernet packet
                 F - IPv4 packet        S - IPv6 packet


            Receiver Sampling Sampling  Maximum Sampling
  Interface   Index    Rate     Direction Header  Types
 ------------ -------- -------- --------- ------- --------
 gi0/1           1      10   rx         128   H


sFlow Pollers Configuration: (Current Tick = 0x002a6476)

sFlow Pollers num:1(limit 864)


 Sampling Types: G - generic counter
                 E - ethernet counter


                    Receiver Sampling
  Interface   Instance Index    Types    Interval
 ------------ -------- -------- -------- --------
 gi0/1           1      1   G          20
```

#On NMS, we can view the ingress flow information of interface

gigabitethernet0/1 on Device.

11.7 LLDP

11.7.1 Overview

11.7.1.1 Overview of LLDP Protocol

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.

11.7.1.2 TLV Type Information

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 1479 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

TLV Type	Description	Whether to release
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 the MAC address of the port.	Yes
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 can be a manually configured IP address, or you can specify an interface and use its IP address as the management address; If not configured, if the port is a routed port, use the IP address configured by its port; If the routed port is not configured, use the loopback interface configured with IP address; If no IP address is configured for	Yes

TLV Type	Description	Whether to release
	any loopback interface, select the primary IP address of the management port of the device; If the management port is not configured, select the primary IP address of the interface allowed to pass through the VLAN; If the primary IP address is not configured for any VLAN, the management address value is blank. The TLV is sent by default.	

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 1480 The description of 802.1 organization-defined TLV

TLV Type	Description	Whether to release
Port VLAN ID TLV	Port VLAN ID	No
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 1481 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 1482 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

TLV Type	Description	Whether to release
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

11.7.1.3 LLDP Work Mechanism

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. If the neighbors reach the threshold, more neighbor advertising packets are dropped and cannot be saved.

11.7.2 LLDP Function Configuration

Table 1483 LLDP function configuration list

Configuration Task	
Configure the LLDP basic functions	Enable the global LLDP function
	Enable the port LLDP function
	Enable LLDP port-based learning neighbor 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 delay of sending packets
	Configure the sending period of packets
	Configure the number of the packets sent fast
	Configure the re-initializing delay
	Configure the period of checking the LLDP configuration

11.7.2.1 Configure LLDP Basic Functions

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 Condition

None

Enable Global LLDP Function

Table 1484 Enable the global LLDP function

Step	Command	Description
Enter the global configuration	configure terminal	-

Step	Command	Description
mode		
Enable the global LLDP function	lldp run	Mandatory By default, do not enable the global LLDP function.

Enable Port LLDP Function

Table 1485 Enable the port LLDP function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet interface/outband management port configuration mode	interface *interface-name*	Either After entering the L2/L3 Ethernet interface/outband management port 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	interface link-aggregation *link-aggregation-id*	
Enable the port LLDP function	lldp enable	Optional By default, Enable the LLDP function on the port.

Enable LLDP Port-based Learning Neighbor Function

After configuring the LLDP port-based learning neighbor function, it can learn and display neighbors based on the single port of the device. By default, the device learns and displays neighbors based on ports and aggregation group ports.

Table 1486 Enable LLDP port-based learning neighbor function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable LLDP port-based learning neighbor function	lldp mode-ap	Optional By default, the function is disabled.

11.7.2.2 Configure LLDP Work Mode

Configuration Condition

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 1487 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	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
Configure the LLDP work mode as Rx	lldp receive	Optional By default, LLDP work mode is RxTx.
Configure the LLDP work mode as Tx	lldp transmit	
Configure the LLDP work mode as RxTx	lldp receive-transmit	

11.7.2.3 Configure TLV LLDP Permits to Release

The neighbor device can get to know the details of the local device by releasing TLV.

Configuration Condition

None

Configure Basic TLV LLDP Permits to Release

The user can release different basic TLVs according to the actual application demand.

Table 1488 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 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	interface link-aggregation *link-aggregation-id*	

Step	Command	Description
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 1489 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 *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	interface link-aggregation *link-aggregation-id*	
Configure the organization-defined TLV LLDP permits to release	lldp tlv-select {dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all | link-aggregation | mac-physic |	Optional By default, permit to release all organization-defined TLVs.

Step	Command	Description
	max-frame-size | power } }	

Configure MED TLV LLDP Permits to Release

The user can release different MED TLVs according to the actual application demand.

Table 1490 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	interface 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.

11.7.2.4 Configure LLDP Parameters

Configuration Condition

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 1491 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 the Delay of Sending Packets

Configuring the delay of sending packets can prevent the frequent change of the local information from causing lots of LLDPDU to be sent.

Table 1492 Configure the delay of sending packets

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the delay of sending the LLDP packets	lldp transmit-delay *transmit-delay-value*	Optional By default, the delay of sending the LLDP packets is 2s.

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 1493 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

Step	Command	Description
		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 1494 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 1495 Configure the re-initializing delay

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the re-initializing	lldp reinit *reinit-*	Optional

Step	Command	Description
delay	*value*	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 1496 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 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	interface link-aggregation *link-aggregation-id*	
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.

11.7.2.5 LLDP Monitoring and Maintaining

Table 1497 LLDP Monitoring and Maintaining

Command	Description
clear lldp neighbors [interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Clear the neighbor information
show lldp neighbors [detail | interface *interface-name* [detail] | interface link-aggregation *link-aggregation-id* [detail]]	Display the neighbor information
show lldp neighbors oui [interface *interface-*	Display the neighbor OUI address information

Command	Description
name | interface link-aggregation *link-aggregation-id*]	and write into Voice-VLAN OUI entry status
clear lldp statistics	Clear the LLDP packet statistics information
show lldp statistics { interface *interface-name* | interface 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 interface 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
show lldp tlv-select [interface *interface-name* | interface link-aggregation *link-aggregation-id*]	Display the basic TLV and organization-defined TLV configuration information
show lldp voice neighbors [detail | interface *interface-name* [detail] | interface link-aggregation *link-aggregation-id* [detail]]	Display the voice neighbor information

11.7.3 LLDP Typical Configuration Example

11.7.3.1 Configure LLDP Basic Functions

Network Requirement

- Configure the LLDP function on Device1, Device2 and Device3, realizing the link-layer neighbor discovery.

Network Topology

Figure 338 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 gigabitethernet0/1 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 gigabitethernet0/1 and gigabitethernet0/2 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 gigabitethernet0/1 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
```

```
1 neighbor entries in system
Capability codes:
      (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
      (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Index       Local Intf            Hold-time  Capability     Peer Intf            Device ID
1             gi0/1                 120        P,R,          gi0/1       Device2
Total entries displayed: 1
```

Device1 discovers neighbor Device2.

#View the details of Device1 neighbor.

```
Device1#show lldp neighbors detail
Neighbor 1:
1. Basic information
Chassis ID                : 0101.7a54.5d0b
Interface ID              : gi0/1
Interface Description         : gigabitethernet0/1
System Name               : Device2
System Description            : SOFOS (R) Operating System Software
Copyright (C) 2013 Sofinet Communication Technology Co.,Ltd.All Rights Reserved.
Time Remaining            : 111 seconds
System Capabilities           : P,R,
Enabled Capabilities          : P,R,
Management Addresses          : IP,10.0.0.1
2. 802.1 organizationally information
Port VLAN ID              : 1
Port And Protocol VLAN ID     : 0
VLAN Name Of VLAN 1           : DEFAULT
3. 802.3 organizationally information
Auto Negotiation              : Supported, Enabled
OperMau                   : Speed(1000)/Duplex(Full)
Port Class                : PSE
PSE Power                 : Supported, Enabled
PSE Pairs Control Ability     : No
Power Pairs               : 1
Power Class               : 1
Link Aggregation              : Supported, Disabled
Link Aggregation ID           : 0
Max Translate Unit            : 1824
4. MED organizationally information
Capabilities              : Not Supported
Class Type                : Not Supported
Application Type              : Not Supported
Policy                    : Not Supported
VLAN Tagged               : Not Supported
```

```
VLAN ID                 : Not Supported
L2 Priority             : Not Supported
DSCP Value              : Not Supported
Location ID             : Not Supported
Power Type              : Not Supported
Power Source            : Not Supported
Power Priority          : Not Supported
Power Value             : Not Supported
HardwareRev             : Not Supported
FirmwareRev             : Not Supported
SoftwareRev             : Not Supported
SerialNum               : Not Supported
Manufacturer Name       : Not Supported
Model Name              : Not Supported
Asset Tracking Identifier   : Not Supported
------------------------------------------
Total entries displayed: 1
```

Note

- For viewing the neighbor information of Device2 and Device3, refer to Device1.

11.8 NDSP

11.8.1 Overview

11.8.1.1 Overview of NDSP Protocol

NDSP (Network Devices Searching Protocol) is a device discovery protocol based on multicast packet, which can discover directly connected devices. It organizes the information of the local device into TLV (type/length/value), which is encapsulated in NDSPPDU (network devices searching protocol data unit) and sent to the directly connected neighbor device. At the same time, it also parses the NDSPPDU received from the neighbor device and caches the information of the directly connected device to the local. Through NDSP, the device can save and manage the information of itself and the directly connected neighbor devices for the network management system to query and judge the communication status of the link.

NDSP has only one table – direct connected neighbor table. For general networks,

there is only one direct connected neighbor on an interface, so the number of table entries will not exceed the number of interfaces.

11.8.2 NDSP Function Configuration

Table 1498 NDSP function configuration list

Configuration task	
Configure NDSP basic functions	Enable the global NDSP function
	Enable the port NDSP function
Configure the LLDP parameters	Configure keepalive time of the neighbor
	Configure the period of sending the packet

11.8.2.1 Configure NDSP Basic Functions

The global NDSP function and port NDSP function must be enabled at the same time so that NDSP can work properly. The local device finds neighbors and obtains neighbor device information by interacting NDSPPDU with other devices.

Configuration Conditions

None

Enable Global NDSP Function

Table 1499 Enable the global NDSP function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the global NDSP function	ndsp run	Mandatory By default, do not enable the global NDSP function.

Enable Port NDSP Function

Table 1500 Enable the port NDSP function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L2/L3 Ethernet	interface *interface-name*	Either

Step	Command	Description
interface configuration mode		After entering the L2/L3 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	Interface link-aggregation *link-aggregation-id*	
Enable the port NDSP function	ndsp enable	Mandatory By default, the port does not enable the NDSP function.

11.8.2.2 Configure the NDSP Parameters

Configuration Conditions

None

Configure Keepalive Time of the Neighbor

TTL is configured to specify the keepalive time of local device information on the neighbor device, so that the neighbor device can delete the local device information after the local device lifetime expires.

Table 1501 Configure the keepalive time of the neighbor

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the keepalive time of the local device on the neighbor device	ndsp holdtime *holdtime-value*	Optional By default, the keepalive time of the local device on the neighbor device is 30s.

Configure the Period of Sending the Packet

By configuring the period of sending the packet, the local device will send the NDSP packet to the neighbor device regularly, so that the information of the local device on the neighbor device will not be aged.

Table 1502 Configure the period of sending the packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the period of sending the NDSP packet	ndsp timer *value*	Optional By default, the period of sending the NDSP packet is 10s.

11.8.2.3 NDSP Monitoring and Maintaining

Table 1503 NDSP monitoring and maintaining

Command	Description
show ndsp neighbors [detail]	Display the neighbor information

11.8.3 NDSP Typical Configuration Example

11.8.3.1 Configure NDSP Basic Functions

Network Requirements

- On Device1 and Device2, configure the NDSP function, realizing the neighbor discovery of the link layer.

Network Topology

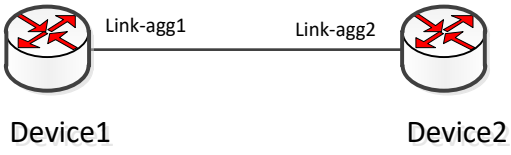


Figure 339 Networking of configuring the NDSP basic functions

Configuration Steps

Step 1: On Device, enable the NDSP function.

#On Device1, enable the NDSP function.

```
Device1#configure terminal
```

```
Device1(config)#ndsp run
```

#On Device2, enable the NDSP function.

```
Device2#configure terminal
Device2(config)# ndsp run
```

Step 2: On the port, configure the NDSP function.

#On port link-aggregation 1 of Device1, enable the NDSP function.

```
Device1(config)# interface link-aggregation 1
Device1(config-if-link-aggregation1)# ndsp enable
```

Device1(config-if-link-aggregation1)#exit

#On port link-aggregation 2 of Device2, enable the NDSP function.

```
Device2(config)# interface link-aggregation 2
Device2(config-if-link-aggregation2)# ndsp enable
Device2(config-if-link-aggregation2)#exit
```

Step 3: Check the result.

#View the neighbor information on Device1.

```
Device1#show ndsp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Interface     Holdtime  Capability  Neighbor Interface    Platform
01017a6a01f2     link-agg1           30        S           link-agg2             SOFOS S3230-28TXF(V1-
switch
```

Device1 discovers the neighbor Device2.

#View the detailed information of the neighbor Device1.

```
Device1#show ndsp neighbors detail
------------------------
Device ID: 01017a6a01f2
Platform: S3230-28TXF(V1)),  Capabilities: Switch
Port: link-agg1,  Port ID (outgoing port): link-agg2
Holdtime : 26 sec


Version :
SOFOS (R) Operating System Software S3230 Software, Version 9.5.0.2(26)(integrity)
RELEASE SOFTWARE Copyright (C) 2019 SOFINET Communication Technology Co.,Ltd.All
Rights Reserved. SOFINET Communication Technology Co.,Ltd.
Compiled Feb 27 2020, 17:00:44
```

Native VLAN : 1

Note

- For the neighbor information of Device2, refer to Device1.

11.9 SNMP

11.9.1 Overview

SNMP (Simple Network Management Protocol) is one standard protocol of managing Internet devices. It ensures that the management information can be transmitted between Network Management 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 Management 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 ISO 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.

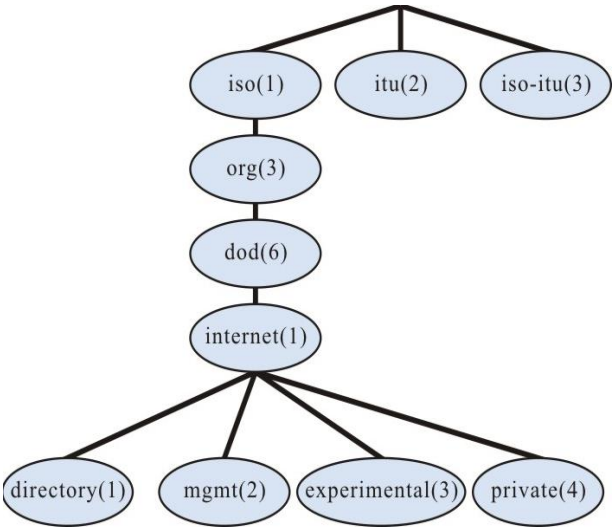


Figure 340 ASN.1 tree diagram of network management

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:

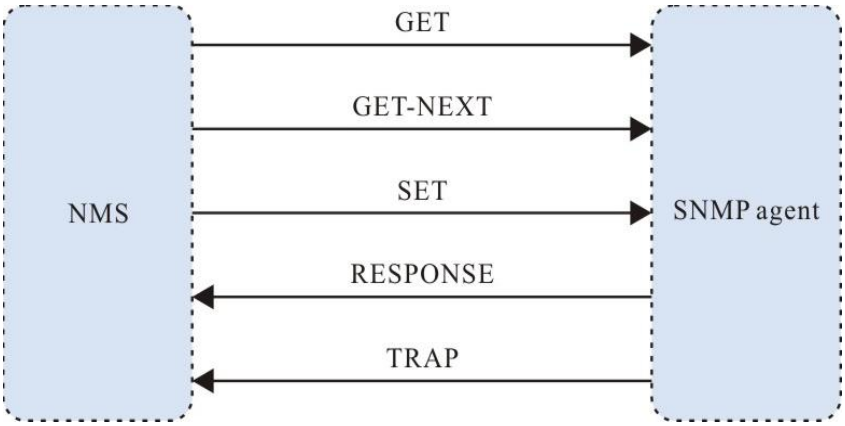


Figure 341 SNMP management operation diagram

- 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 1504 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.

11.9.2 SNMP Function Configuration

Table 1505 SNMP function configuration list

Configuration Task	
Configure the SNMP basic functions	Enable the SNMP service
	Configure the MIB view

Configuration Task	
	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
	Configure the SNMP user
	Configure SNMP advertising
	Configure SNMP agent forwarding

11.9.2.1 Configure SNMP Basic Functions

Configuration Condition

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 1506 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 1507 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 the system startup time type got in MIB	snmp-server mib2 sysuptime { snmp-agent-uptime | system-uptime }	Mandatory By default, it is system-uptime.

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 1508 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 1509 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

11.9.2.2 Configure SNMPv1/v2

Configuration Condition

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 1510 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* | *access-list-name*]	Mandatory By default, the community name is public.

11.9.2.3 Configure SNMPv3

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 1511 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, SHA), authentication password, encryption algorithm (DES), and encryption password.

Table 1512 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| SM3 } *password* [encrypt {des | aes | SM4 } *password*]] [access *access-list-number* | access-list-name | *Ipv6 access-list-number*]	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 1513 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

Step	Command	Description
		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 1514 Configure the proxy forwarding

Step	Command	Description
Enter the global configuration mode	config terminal	-
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

11.9.2.4 Configure SNMP Trap

Trap is the information that SNMP agents actively send to network workstations to report specific events. Trap packets can be divided into general Trap and custom Trap. General Trap includes Authentication, Linkdown, Linkup, Coldstart, Warmstart, crc-error, out-packet-error, out-usage-rate, in-packet-error, and in-usage-rate. Custom Trap is output according to the requirements of each module.

Table 1515 Configure Trap

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the trap of the link interface down or up	snmp-server enable traps snmp [linkup | linkdown]	Mandatory By default, SNMP Trap is disabled.
Enter the interface configuration mode	interface *interface-type interface-num*	Optional
Configure the trap of the interface status change	snmp trap link-status	Optional
Configure 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*]	Mandatory It is necessary to specify ip-address as the IP address of the network work station.
Configure the source address of the Trap packet	snmp-server trap-source *ip-address*	Optional

Note

- Usually, there is much Trap information, so it will occupy equipment resources and affect equipment performance. Therefore, it is recommended that the Trap function of specified modules be enabled as

needed, not all modules are enabled.

11.9.2.5 SNMP Monitoring and Maintaining

Table 1516 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
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 port	Display the port number configured by the SNMP protocol
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

Command	Description
	information
show snmp-server user	View the SNMP user information
show snmp-server view	View the SNMP view information

11.9.3 SNMP Typical Configuration Example

11.9.3.1 Configure SNMP v1/v2c Proxy Server

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 342 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 common 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, emvironment overtemperature alarm. Device generates the corresponding Trap information and sends to NMS.

11.9.3.2 Configure SNMP v3 Proxy Server

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 343 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 admin encrypt 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.

11.9.3.3 Configure SNMP v3 trap Notify

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 344 Networking of configuring SNMPv3 trap notify

Configuration Steps

Step 1: Configure the IP address of the interface. (Omitted).

Step 2: Enable the SNMP proxy on Device and configure the SNMPv3 basic information.

#Configure Device.

Enable SNMP proxy; configure the node view name as default, and you can access all objects in the access 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 user group as public, security level as authpriv, read-write view and notify view all use 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 common Trap information.

```
Device(config)#snmp-server enable traps
```

Step 3: Configure Device to send SNMP v3 trap packet to NMS.

#Configure Device.

Configure SNMP v3 trap user name as public on NSM, and the security level as authpriv.

```
Device(config)#snmp-server host 129.255.140.1 version 3 user public
authpriv version 3
```

Step 4: Configure NMS.

#On NMS, it is necessary to configure the user name and password consistent with SNMP proxy, run network management software and monitor UDP 162 port number.

Step 5: Check the result.

#NMS can receive various kinds of Trap information from Device, such as route change caused by Device interface up and down, environment overtemperature alarm. Device will generate corresponding Trap information and send it to NMS.

11.9.3.4 Configure SNMP v3 inform Notify

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 345 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.

#You need to set the user name and select the security level when using NMS of SNMP V3 version. According to different security levels, it is necessary to set authentication algorithm, authentication password, encryption algorithm, encryption password, etc., and monitor UDP port number 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.

11.9.3.5 Configure SNMP v3 Proxy Forwarding

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 346 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 authpriv; 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 proxy, encryption algorithm as DES, and encryption password as proxy.

```
Device1(config)#snmp-server group group-local v3 authpriv read default write default notify default
```

```
Device1(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 800016130301017a000137
```

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 800016130301017a000137, 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 800016130301017a000137 plocal tuser proxyuser
Device2(config)#snmp-server context proxyuser
```

#View the engineID information of Device2.

```
Device2#show snmp-server engineID
Local  engine ID: 8000161303000000052fd
IPAddress: 150.1.2.2 remote port: 161 remote engine ID: 800016130301017a000137
```

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.

11.10 RMON

11.10.1 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;
- capture: The captured groups set up one group of buffer area, used to store the groups captured from the channel.
- 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

11.10.2 RMON Function Configuration

Table 1517 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

11.10.2.1 Enable RMON Function

Configuration Condition

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 1518 Enable the RMON function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the RMON function	rmon	Mandatory

11.10.2.2 Configure RMON Alarm Group

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 Condition

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 1519 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.

11.10.2.3 Configure RMON Extended Alarm Group

RMON extended alarm group can calculate the alarm variable, and then, compare the calculation result with the set threshold value, realizing the richer alarm function.

Configuration Condition

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 one statistics group

Configure RMON Alarm Group

Table 1520 Configure the RMON alarm group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the RMON function	rmon	Optional
Configure one statistics group	rmon statistics ethernet *statistics-num OID* [owner *owner*]	Mandatory By default, the owner of the statistics group is config.
Configure 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*]	Mandatory By default, the owner of the alarm group is config.

11.10.2.4 Configure RMON Event Group

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 Condition

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 1521 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.

11.10.2.5 Configure RMON History Event

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 Condition

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 1522 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.

11.10.2.6 Configure RMON Statistics Group

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 Condition

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 1523 Configure RMON statistics management function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the RMON function	rmon	Mandatory

Step	Command	Description
Configure the RMON statistics group	rmon statistics ethernet *statistics-num OID* [owner *owner*]	Mandatory By default, the owner of the statistics group is config.

11.10.2.7 RMON Monitoring and Maintaining

Table 1524 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 prialarm	Display the RMON extended alarm configured in the device
show rmon statistics ethernet	Display the RMON statistics group configured in the device

11.10.3 RMON Typical Configuration Example

11.10.3.1 Configure RMON Basic Functions

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 347 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 common 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. You can use the **show interface switchport snmp ifindex** command to display the snmp index values of all L2 ports; the **show interface snmp ifindex** command displays the snmp index value of all L3 ports; the **show interface switchport XXXX snmp ifindex** command displays the snmp index value of the specified L2 port; the command **show interface XXXX snmp ifindex** displays the snmp index value of the specified L3 port.
- 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#show 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.

11.11 CWMP

11.11.1 Overview

CWMP (CPE WAN Management Protocol) is a protocol developed by the BroadBandForum.org to manage and configure the CPE (Customer Premise Equipment), also called TR-069. It defines the general protocol frame, message standard, management mode, and data model to manage the CPE connecting to the carrier's Internet broadband access network.

CWMP can be described as a data frame model, which describes the communication between the device such as broadband router and the ACS (Auto-Configuration Server). It is used to perform the remote centralized configuration and management to the CPE (such as broadband router, switch, Internet gateway device, and STB) from the user side.

CWMP protocol is an application layer protocol above the IP layer. This protocol can be applied widely and has no restrict on the access mode. CPEs based on the following access modes, such as ADSL- (Asymmetrical Dig2wital Subscriber Loop),

Ethernet network, and PON (Passive Optical Network), can use this protocol. System architecture based on the TR069 is shown in Figure 10-1. End-to-end architecture of the CWMP protocol has the following features:

With elastic connection model, both the CPE and ACS can trigger the connection establishment. This avoids maintaining connection between the CPE and ACS.

It can be automatically discovered between the CPE and ACS.

ACS can dynamically configure and monitor the CPE.

For the CPE, the CWMP mainly completes the following four aspects of work:

1. Configure the CPE automatically and configure the dynamic service. For the ACS, each CPE can mark itself in the protocol, such as the model and version. According to the set rule, the ACS can send the configuration to a certain CPE or to a group of CPEs. The CPE can automatically request the ACS configuration information when it powers on and the ACS can actively initiate the configuration at any time. Through this function, it can achieve the CPE "zero configuration installation" function or control the service parameter dynamic change from the network side.
2. Manage the version file and configuration file of the CPE. The CWMP provides the management and download to the version file and configuration file in the CPE. The ACS can identify the version number of the user device and determines whether to remote update the software version of the device. The ACS can know whether the update succeeds after update completes. The CPE can backup through uploading the configuration file and recover through downloading the configuration file under the ACS control.
3. Configure remote upgrade to the CPE. It is a function initiated by the ACS to configure the remote upgrade to the CPE. Currently, the ACS performs remote upgrade to the CPE configuration in the hierarchical mode.
4. Achieve the secure management to the device interface. Through the RPC

mode defined by the CWM (remote process invoking), it can perform secure management to the device interface, including the disabling, enabling, automatic binding, automatic unbinding, 802.1x interface, and disabling the 802.1x function

Warning

- Ensure that the device with Flash as 16M will not power off or reboot when upgrading the version using the CWMP and ensure the correctness of the upgrade version. Otherwise, the system may fail to be booted.

Note

- When the device works in the VST mode, the device does not support the CWMP function.

11.11.2 CWMP Function Configuration

Table 1525 CWMP function configuration list

Configuration Task	
Configure the CWMP basic function	Enter the CWMP configuration mode
	Enable the CWMP proxy
	Configure the ACS server related information
	Configure the WAN device interface
	Configure the CWMP to periodically send the INFORM packet
	Configure the period of the CWMP sending the INFORM packet
	Configure the CWMP file download
	Configure the breakpoint resume function of the CWMP file
	Configure the provision code of the CWMP
Configure the CWMP authentication and	Configure the CWMP authentication information

Configuration Task	
encryption function	Configure the ACS certificate of the CWMP
	Configure the ACS certificate fingerprint of the CWMP
Configure the CWMP extended function	Configure the specified IP address of the CWMP
	Configure the CWMP link backup

11.11.2.1 Configure CWMP basic function

Configuration Condition

Before configuring the CWMP proxy basic function, first enter the global configuration mode and then configure the CWMP proxy basic function.

Enter CWMP Configuration Mode

For the configuration related to the CWMP proxy, first enter the CWMP proxy configuration mode.

Table 1526 Enter the CWMP configuration mode

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory

Enable CWMP Proxy

If the device is enabled with the CWMP proxy function, then the device can interact with the CS through the CWMP proxy to remote configure and manage the device.

Table 1527 Enable the CWMP proxy

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory

Step	Command	Description
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is in the disabled state.

Configure ACS Server Related Information

By configuring the ACS related information, including the connection address of the ACS server, the device can communicate with the ACS server.

Table 1528 Configure the ACS server related information

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is in the disabled state.
Configure ACS related information	management server url *url-string*	Mandatory By default, the device is not configured with the ACS related parameter. For the unencrypted mode, *url-string* uses the http protocol. For the encryption mode, *url-string* uses the https protocol.
Configure the user name of the device initiating the connection to the ACS	management server *user-name*	Optional By default, the device is not configured with the ACS related parameter. If the user name is not configured on the ACS, do not need to configure the user name.

Step	Command	Description
Configure the user name and corresponding password of the device initiating the connection to the ACS	management server *password*	Optional By default, the device is not configured with the ACS related parameter. If the user name and corresponding password are not configured on the ACS, do not need to configure the user name and password.

Configure WAN Device Interface

Specify the interface as the default WAN device interface in the interface mode. If the default WAN device is not specified, it will cause that the CWMP proxy cannot send the Inform packet to connect the ACS server.

Table 1529 Configure the WAN device interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L3 interface to be used	interface *interface-name*	Mandatory It must be configured in the L3 interface mode.
Configure the default WAN device	cwmp wan default	Mandatory By default, the WAN device interface of the CWMP proxy is not specified.

Note

- If the default WAN device is not specified, it may cause that the CWMP cannot send the Inform packet to connect the ACS. It must be clear that the parameter name and the IP address of the WAN device connecting

to the Internet in the current system when organizing the Inform packet.

- After an interface is specified as the default WAN device, if the WAN IP address is not configured in the CWMP mode and the interface is configured with the IP address, the connection request URL is generated by using the IP address of the interface.

Configure CWMP to Periodically Send INFORM Packet

By configuring the CWMP to periodically send the Inform packet, the device can periodically send the Inform packet to the ACS. After the ACS receives the Inform packet sent by the device, handle the packet based on the pre-configuration.

Table 1530 Configure the CWMP to periodically send the INFORM packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP to periodically send the INFORM packet	enable inform	Mandatory By default, the function of CWMP periodically sending the INFORM function is enabled.

Configure Period of CWMP Sending INFORM Packet

After configuring the CWMP to periodically send the INFORM packet, you can configure the period of the CWMP proxy sending the Inform packet. The default sending period is 43200s (12h).

Table 1531 Configure the period of the CWMP sending the INFORM packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP to periodically send the INFORM packet	enable inform	Mandatory By default, the function of the CWMP periodically sending the INFORM packet is enabled,
Configure the period of the CWMP sending the INFORM packet	inform interval *inform-interval*	Mandatory By default, the interval for the device automatically sending the inform packet is 43200s.

Note

- After the function of the CWMP proxy sending the Inform packet is configured and the sending period of the Inform packet is not configured, the CWMP sends the Inform packet to the ACS in 43200s (12h) by default.
- After the periodical sending interval of the Inform packet is modified, the modified interval can only take effect when the last interval expires. If you want the modified interval to take effect immediately, you can reboot the CWMP proxy. Wherein, for enable and no enable, refer to the related chapter in the CWMP command manual.

Configure CWMP File Download

When the function of CWMP proxy supporting the file download is required to

download the version file and configuration file, configure the CWMP proxy file download function in advance.

Table 1532 Configure the CWMP file download

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP file download function	enable download	Mandatory By default, the file download function of the CWMP is not enabled.

Configure Breakpoint Resume Function of CWMP File

After the CWMP file download function is configured and the CWMP is required to support the breakpoint resume function, you can configure the function.

Table 1533 Configure the breakpoint resume function of the CWMP file

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP file download function	enable download	Mandatory By default, the file download function of the CWMP is not enabled.
Configure the breakpoint	enable download resume	Mandatory

Step	Command	Description
resume function of the CWMP file		By default, the file breakpoint resume function of the CWMP is not enabled.

Note

- Before the breakpoint resume function of the CWMP file is configured the file download function of the CWMP must be configured. If the file download function is not configured at first, then the file breakpoint resume function will not take effect even if the file resume function is configured.

Configure CWMP Provision Code

This function is used to configure the CWMP provision code which is used to mark the basic service information provided by the CWMP.

Table 1534 Configure CWMP provision code

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the CWMP provision code	provision code *provision-code*	Mandatory By default, the CWMP is not configured with the provision code.

11.11.2.2 Configure CWMP Authentication and Encryption Function

Configuration Condition

Before configuring the CWMP authentication and encryption function, first complete the following task:

- The basic configuration of the CWMP proxy is completed, including the CWMP proxy enabling configuration and the ACS information configuration of the CWMP proxy.
- When configuring the encryption function, prepare the certificate and it requires manual import.

Configure CWMP Authentication Function

When the ACS requires initiating the connection to the device, configure the CWMP proxy to authenticate the connection request sent from the ACS in terms of the security.

Table 1535 Configure the CWMP authentication function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the user name for the CPE authenticating the connection request from the ACS	connection request username *user-name*	Optional By default, the user name is not configured.
Configure the password for the CPE authenticating the	connection request password *password*	Optional By default, the password is not

Step	Command	Description
connection request from the ACS		configured.

Configure CWMP PKI Trust Domain Name

Viewing from the security, when the device connects to the ACS through the HTTPS mode, you need to specify the KPI trust domain name of the CWMP proxy, so as to verify the validity of the ACS certificate.

Table 1536 Configure the CWMP ACS certificate

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the KPI trust domain name of the CWMP proxy	secure-identity ca-*name*	Mandatory By default, the CWMP proxy does not have the KPI trust domain name.

11.11.2.3 Configure CWMP Extended Function

Configuration Condition

Before configuring the CWMP extended function, first complete the following tasks:

- Complete the CWMP basic configurations, including the CWMP proxy enabling configuration, CWMP proxy ACS information configuration.
- Configure the IP address of the interface to enable that the network layers of the neighboring nodes are reachable.
- When the link backup function is required, the interface configured as

backup must be normal, including the configured IP address and the interface in the UP state.

Configure CWMP Specified Source IP Address

When the source IP address is configured, the ACS can directly communicate with the specified IP address.

Table 1537 Configure the source IP address specified by the CWMP

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the CWMP proxy configuration mode	cwmp agent	Mandatory
Enable the CWMP proxy	enable	Mandatory By default, the CWMP proxy is disabled.
Configure the source IP address specified by the CWMP proxy	ip source *ip-address*	Mandatory By default, the source IP address of the packet is not specified when the device establishes link with the ACS and the source IP address of the packet is the packet egress interface.

Configure CWMP link backup

When the link backup function is configured under the interface mode, there is one default WAN interface and others are backup WAN interfaces when the device is configured with multiple WAN interfaces. The IP address of the default WAN interface is used to generate the connection request URL and then send it to the ACS. When the default WAN interface is down, one interface is chosen from the backup WAN interface and is considered as the current WAN interface. Then, its IP address is used to generate the connection request URL,

Table 1538 Configure the CWMP link backup

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the L3 interface requiring setting backup	interface *interface-name*	Mandatory
Configure the backup interface of CWMP proxy	cwmp wan backup	Mandatory By default, the WAN device backup interface of the CWMP proxy is not specified.

Note

- Each device can only be configured with one CWMP WAN default interface and one CWMP WAN backup interface.

11.11.2.4 CWMP Monitoring and Maintaining

Table 1539 CWMP monitoring and maintaining

Command	Description
show cwmp agent	Display the related information of the CWMP proxy.
show cwmp session	Display the session information of the CWMP proxy.
show cwmp methods	Display the RPC (Remote Procedure Call)) supported by the CWMP proxy
show cwmp parameter all	Display all the parameter names of the CWMP proxy
show cwmp parameter *para-string*	Display the detailed parameter information of the specified CWMP proxy
show cwmp parameter notify { active | all | forceactive | passive }	Display the notified parameter name of the CWMP proxy
show cwmp parameter values [*para-string* |	Display the detailed parameter information of

Command	Description
error]	the specified CWMP proxy

11.11.3 CWMP Typical Configuration Example

11.11.3.1 Configure CWMP Authentication Function

Network Requirements

- Device visits the ACS through the Network and enable the CWMP function on Device. Configure the authentication function both on Device and ACS.
- After the authentication passes, Device will execute the version upgrade, configuration restoration, configuration backup, and configuration upgrade tasks sent by the ACS.

Network Topology

Figure 348 Networking of the CWMP authentication function

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. (Omitted)

Step 3: Configure the CWMP.

#Enable the CWMP proxy and file download function on Device and configure the URL of the ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url https://129.255.136.200:8409/acs
```

```
Device(config-cwmp)#enable download
Device(config-cwmp)#exit
```

#Configure the VLAN2 interface as the default WAN device.

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#cwmp wan default
Device(config-if-vlan2)#exit
```

Step 4: Configure the ACS server.

#Create the fragment template on the ACS and configure both the authentication user name and password as admin. (Omitted)

#Create the configuration upgrade task on the ACS and choose the fragment template to be created. Deliver the configuration task to Device. (Omitted)

Note

- The ACS sends the authentication user name and password to Device through configuring the upgrade task to ensure that the ACS can pass the Device authentication.

#Create version upgrade task, restoration task, and backup task on the ACS.

Step 5: Check the result.

#Execute the show running-config command on Device and it can be viewed that the ACS sends the user name and password of Device.

```
cwmp agent
 management server url https://129.255.136.200:8409/acs
 connection request username admin
 connection request password admin
 enable download
 enable
 exit
```

#Device can successfully execute the version upgrade task. Configure the restoration task and backup task sent by the ACS.

11.11.3.2 Configure Source IP Address specified by CWMP

Network Requirements

- Device visits the ACS through Network and enable the CWMP function on Device.
- Specify the source IP address of the CWMP as 1.0.0.1. enable Device to visit the ACS through the firewall and execute the version upgrade, configuration restoration, and configuration backup tasks sent by the ACS.

Network Topology

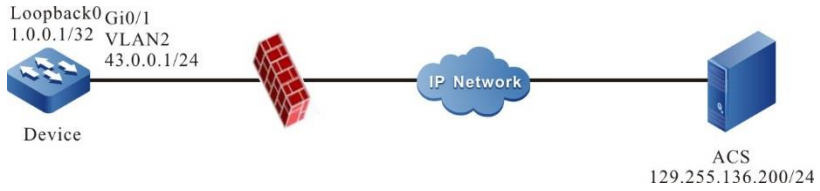


Figure 349 Networking of configuring the source IP address specified by the CWMP

Configuration Steps

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

Step 2: Configure the IP address and router of the interfaces. (Omitted)

Step 3: Configure the CWMP.

Enable the CWMP proxy and file download function on Device. Configure the URL of the ACS and the source IP address of the CWMP as 1.0.0.1.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url https://129.255.136.200:8409/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#ip source 1.0.0.1
Device(config-cwmp)#exit
```

#Configure the Loopback0 interface as the default WAN device.

```
Device(config)#interface loopback 0
Device(config-if-loopback0)#cwmp wan default
Device(config-if-loopback0)#exit
```

Step 4: Configure the firewall.

#The firewall rejects the packet with the source IP address as 43.0.0.1 to pass and allows the packet with the source IP address as 1.0.0.1 to pass.

Step 5: Configure the ACS server.

#Create the version upgrade task and configuration restoration task and configuration backup task on the ACS.

Step 6: Check the result.

#Execute the show running-config command on Device and the configured source IP address can be viewed.

```
cwmp agent
 management server url https://129.255.136.200:8409/acs
 enable download
 enable
 ip source 1.0.0.1
 exit
```

#Device can successfully execute the version upgrade task and configuration restoration task and configuration backup task sent by the ACS.

11.11.3.3 Configure CWMP Link Backup

Network Requirements

- Device can visit the ACS through two links. The gigabitethernet0 interface is selected by priority to communicate with the ACS.
- When the vlan2 interface is faulty, Device can communicate with the ACS through the vlan3 interface. When the gigabitethernet0 interface recovers, Device can communicate with the ACS through the vlan2 interface.

Network Topology

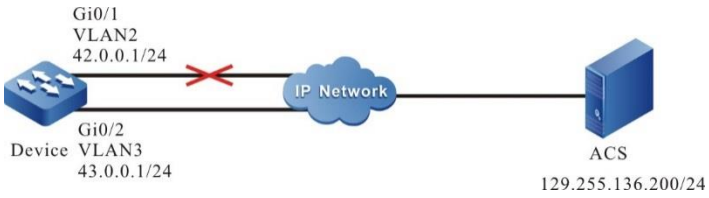


Figure 350 Networking of configuring the CWMP link backup

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 interfaces. (Omitted)

Step 3: Configure the CWMP.

#Enable the CWMP proxy and file download function on Device and configure the URL of the ACS.

```
Device#configure terminal
Device(config)#cwmp agent
Device(config-cwmp)#enable
Device(config-cwmp)#management server url https://129.255.136.200:8409/acs
Device(config-cwmp)#enable download
Device(config-cwmp)#exit
```

#Configure the vlan2 interface as the default WAN interface.

```
Device(config)#interface vlan2
Device(config-if-vlan2)#cwmp wan default
Device(config-if-vlan2)#exit
```

#Configure the vlan3 interface as the backup WAN device.

```
Device(config)#interface vlan3
Device(config-if-vlan3)#cwmp wan backup
Device(config-if-vlan3)#exit
```

Step 4: Check the result.

#View the CWMP proxy information on Device.

```
Device#show cwmp agent
 Agent status: Enabled
 Periodic Inform: Enabled
```

Download files: Enabled
Inform interval: 43200
ACS URL: https://129.255.136.200:8409/acs
ACS user name:
ACS user password:
Connection request URL: http://42.0.0.1:7547/01017A/SFN3300/01017a136922/cwmp
Connection request user name:
Connection request password:
Default WAN device: vlan2
Current WAN device: vlan2
CA certificate: /flash/tr069/ca.pem

It can be viewed that the default WAN device is VLAN2 and current WAN device is VLAN2. It can be viewed on the ACS management page that the corresponding IP address of Device is 42.0.0.1.

#When the VLAN2 interface on Device is faulty, view the CWMP proxy information.

Device#show cwmp agent
Agent status: Enabled
Periodic Inform: Enabled
Download files: Enabled
Inform interval: 43200
ACS URL: https://129.255.136.200:8409/acs
ACS user name:
ACS user password:
Connection request URL: http://43.0.0.1:7547/01017A/SFN3300/01017a136922/cwmp
Connection request user name:
Connection request password:
Default WAN device: vlan2
Current WAN device: vlan3
CA certificate: /flash/tr069/ca.pem

It can be viewed that the default WAN device is vlan2 and current WAN device is vlan3. It can be viewed on the ACS management page that the corresponding IP address of Device is 43.0.0.1.

#When the vlan2 interface on Device is recovered, view the CWMP proxy information. It can be viewed that both the default WAN device and the current WAN device is vlan2. It can be viewed on the ACS management page that the corresponding

IP address of Device is 42.0.0.1.

11.12 NETCONF

11.12.1 Overview

NETCONF (Network Configuration Protocol) is a kind of network management protocol based on XML. It provides a programmable method to configure and manage network devices. With this protocol, users can set parameters, obtain parameter values, obtain statistical information, etc. NETCONF packet uses the XML format and has powerful filtering ability. Each data item has a fixed element name and location, which makes different devices of the same manufacturer have the same access mode and result presentation mode. The devices of different manufacturers can also get the same effect by mapping XML, which makes it very convenient in the development of the third-party software, it is easy to develop a special customized network management software in the environment of mixing different manufacturers and different devices. With the help of such network management software, using NETCONF function will make the configuration management of network equipment simpler and more efficient.

11.12.2 NETCONF Basic Function Configuration

Table 1540 NETCONF basic function configuration list

Configuration Tasks	
Configure the functions of the NETCONF server	Enable the NETCONF server function
	Configure the NETCONF server to bind the IPv4 and IPv6 standard ACL
	Configure the DSCP value of the network packet of the NETCONF server
	Configure the NETCONF server not to synchronize the data
	Configure the disconnection timeout of the NETCONF client
	Configure the maximum sessions of NETCONF
Configure the NETCONF CALL-HOME	Configure the NETCONF CALL-HOME

Configuration Tasks	
function	function

11.12.2.1 Configure NETCONF Server Functions

Configuration Conditions

Before configuring the functions of the NETCONF server, first complete the following tasks:

- Configure the link-layer protocol and ensure the normal communication of the link layer.
- Configure the network-layer address of the interface and ensure that the NETCONF client node is reachable at the network layer.

Enable NETCONF Server Function

Table 1541 Enable the NETCONF server function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the global NETCONF function	netconf server enable[port *port-number*]	Mandatory By default, the NETCONF function is not enabled. The monitor port of the NETCONF server is 830.

Configure NETCONF Server to Bind IPv4 and IPv6 Standard ACL

Table 1542 Configure the NETCONF server to bind the IPv4 and IPv6 standard ACL

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the NETCONF server to bind the IPv4 and IPv6 standard ACL	netconf server access-class { ipv4 | ipv6 } { *access-list-number* | *access-list-name* }	Mandatory By default, the NETCONF server is not configured to bind the IPv4 and IPv6 standard

Step	Command	Description
		ACL.

Configure the DSCP Value of the Network Packet of NETCONF Server

Table 1543 Configure the DSCP value of the network packet of the NETCONF server

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the DSCP value of the network packet of the NETCONF server	netconf server dscp *dscp-value*	Mandatory By default, the DSCP value of the network packet of the NETCONF server is 48.

Configure NETCONF Server Not to Synchronize Data

Table 1544 Configure the NETCONF server not to synchronize data

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the NETCONF server not to synchronize data	netconf server without-data-sync	Mandatory By default, the NETCONF server will not synchronize data to the controller.

Configure Timeout Disconnection Function of the NETCONF Client

Table 1545 Configure the timeout disconnection time of the NETCONF client

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the global NETCONF function	netconf client idle-time	Mandatory By default, the timeout disconnection time of the NETCONF client is 3600s.

Configure Max. Sessions of NETCONF

Table 1546 Configure the maximum number of the NETCONF sessions

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the maximum sessions of NETCONF	netconf server max-session session-num	Optional By default, the maximum sessions supported by the NETCONF server is 4.

11.12.2.2 Configure NETCONF CALL-HOME Function

Configuration Conditions

Before configuring the NETCONF server function, first complete the following tasks:

- Configure the link-layer protocol and ensure the normal communication of the link layer.
- Configure the network-layer address of the interface and ensure that the NETCONF client node is reachable at the network layer.

Configure NETCONF CALL-HOME Function

The configured call-home terminal can automatically connect to the configured terminal after NETCONF service is enabled, so as to establish an SSH connection of NETCONF without the client actively connecting to the NETCONF server.

Table 1547 Configure NETCONF CALL-HOME function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure NETCONF CALL-HOME function	netconf call-home client *client-name* ssh *endpoint-name* address *host-name* [port *port-number* / dscp *dscp-value* / vrf *vrf-name* / source-interface	Mandatory By default, there is no call-home termimal.

Step	Command	Description
	source-interface-name]	

11.12.2.3 NETCONF Monitoring and Maintaining

Table 1548 NETCONF monitoring and maintaining

Command	Description
debug netconf [all | cmf | conf | database | dbm | plugin | server | ssh | yang]	Open the NETCONF debug switch
clear netconf session *session-id*	Clear the specified NETCONF client connection session ID
show netconf session	Display the connected session information of the NETCONF client

11.12.3 NETCONF Typical Configuration Example

11.12.3.1 Configure NETCONF Server

Network Requirements

- Device1 and device2 are NETCONF server devices, which connect with the controller through unicast routing protocol.
- The controller monitors and manages device1 and device2 through NETCONF.

Network Topology

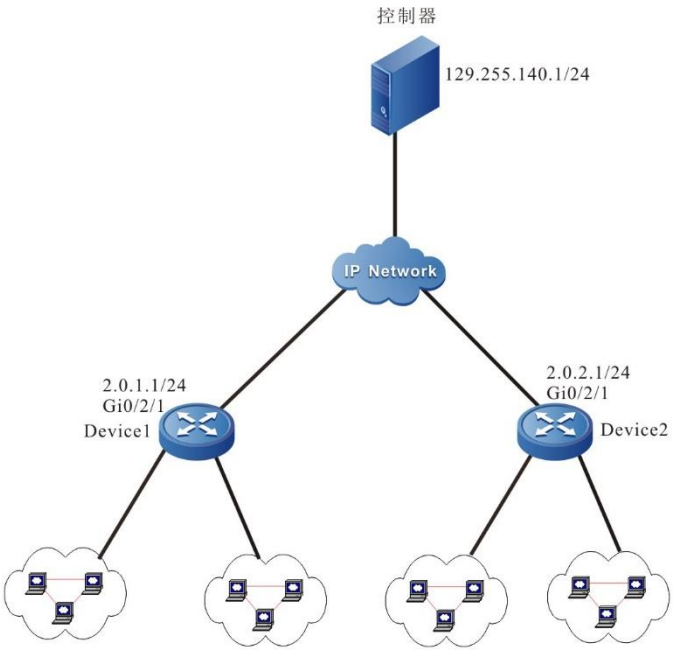


Figure 351 Networking of configuring NETCONF server

Configuration Steps

Configure the controller and the device to extablish the NETCONF connection, and then the controller configures and manages the device through NETCONF. Take Device1 as an example, and the configuration of Device2 is similar and will not be repeated.

Step 1: Configure the IP address of the interface (omitted).

Step 2: Configure the NETCONF user.

#Create a netconf user with the user name admin and password admin@123 on the device.

```
Device1#configure terminal
Device1(config)#local-user admin class manager
Device1(config-user-manager-admin)#service-type netconf ftp
Device1(config-user-manager-admin)#password 0 admin@123
Device1(config-user-manager-admin)#privilege 15
Device1(config-user-manager-admin)#exit
```

Step 3: Configure the device to enable the NETCONF server function.

#On the device, configure to enable the NETCONF server function.

```
Device1(config)#netconf server enable
```

Step 4: Configure the controller.

#Open the controller, click "Network Plan", select "Network Discovery", click "Add Node", configure NETCONF parameters: "IP Address", "Name", "Account" and "Password", in which the configured parameters "IP Address", "Account" and "Password" must be consistent with those on the device. Click OK and the normal communication between the device and the controller is set up.

Step 5: Check the result.

#Query the connection between the controller and the NETCONF server of the device.

```
Device1#show netconf session
------------------
session id: 1
transport: SSH
user name: admin
source host: 129.255.140.1
login time: 2019-06-1T20:29:05Z
in rpcs: 1
in bad rpcs: 0
out rpc errors: 0
out notifications: 0
```

11.13 Telemetry

11.13.1 Overview

Telemetry is a technology of collecting data from network devices remotely with a high speed. It uses "push mode" to timely obtain rich monitoring data of the network devices, so as to quickly realize network fault location and efficient intelligent operation and maintenance of the network.

With the increasing scale of the network and the low management efficiency of traditional network monitoring methods (such as SNMP and CLI), it cannot meet the needs of high-performance network monitoring. After the emergence of the Telemetry

technology, it can achieve higher precision and more real-time monitoring data collection for large-scale networks, and quickly locate and solve network problems, so that it provides an important big data platform for network quality optimization, and provides a strong support for the requirements and development of intelligent network operation and maintenance in the future.

The telemetry function mainly includes two parts:

- Static subscription

Telemetry static subscription indicates that the device acts as the client, the collector acts as the server, and the device actively initiates the connection to the collector for data collection and submission

- Dynamic subscription

Telemetry dynamic subscription indicates that the device acts as the server, the collector acts as the client to initiate he connection to the device, and the device collects and transmits data.

11.13.2 Telemetry Function Configuration

Table 1549 Telemetry function configuration list

Configuration Tasks	
Configure Telemetry static subscription function	Configure the sensor
	Configure the collector
	Configure subscription
	Enable subscription
Configure Telemetry dynamic subscription function	Configure the GRPC server

11.13.2.1 Configure Telemetry Static Subscription Function

Configuration Conditions

None

Configure Sensor

When configuring the Telemetry static subscription sampling data, you need to create a sampling sensor group, and then specify the sampling path for transmitting data. In addition, when it is necessary to configure the sampling path with filtering conditions, you can specify the corresponding condition expression through condition configuration, that is, transmit the data when meeting the conditions of the expression.

Table 1550 Configure the sensor

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the sensor group mode	telemetry sensor-group *sensor-name*	Mandatory If the group does not exist, directly create a group and enter the group mode. Otherwise, directly enter the group mode.
Configure the sensor path	sensor-path path-name { [condition-express op-field field op-type op op-value value [{ and | or } op-type op op-value value]] }	Mandatory

Configure Target Collector

When configuring the Telemetry static subscription sampling data, you need to create a delivery target group, and then specify the target collector to which the sampling data is delivered.

Table 1551 Configure the target collector

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the sensor group mode	telemetry destination-group	Mandatory

Step	Command	Description
	destination-name	If the group exists, directly enter the group mode.
Configure the target address	ipv4-address [vrf vrf-name] *ip-address* port *port-num*	Mandatory By default, vrf uses global, and the value range of port is 1-65535.

Create Subscription

When configuring the Telemetry static subscription to sample data, you need to create a subscription to associate the configured delivery target group with the sampling sensor group, and complete the data delivery.

Table 1552 Create subscription

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the subscription group mode	telemetry subscription *subscription-name*	Mandatory
Configure the sending source interface of the subscription	source-interface *interface-name*	Optional By default, the outgoing interface for transmission will be determined according to the route, and the active IP address of the outgoing interface will be used as the source IP address for transmission
Configure to associate the sensor group	sensor-group *sensor-name* [sample-interval *sample-interval*]	Mandatory If the sensor group does not exist, you need to configure the sensor group first. The default value of sample-interval is 10000 milliseconds
Configure associated	destination-group *destination-*	Mandatory

Step	Command	Description
delivery target group	*name*	If the target group does not exist, you need to configure the delivery target group first.
Enable subscription	subscription enable	Mandatory After enabling, complete the data delivering.

11.13.2.2 Configure Telemetry Dynamic Subscription Function

Configuration Conditions

None

Enable GRPC Server

For dynamic subscription, the device side acts as a server, so enable the GRPC server function of the device. If you need to complete the dynamic subscription data submission, you need to establish a connection between the collector as a client and the device.

Table 1553 Configure GRPC server

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the GRPC server	grpc server [port port-*num*]	Mandatory The default value of port is 51700.

11.13.2.3 Telemetry Monitoring and Maintaining

Table 1554 Telemetry monitoring and maintaining

Command	Description
show telemetry sensor-group [*sensor-name*]	Display the sampling sensor information, including the configured sampling path

Command	Description
	information
show telemetry destination [*destination-name*]	Display the delivery target group information, including the configured delivery target address information
show telemetry subscription [*subscription-name*]	Display the subscription information, including the configured associated sensor group and target group information
show telemetry sensor-path	Display the sampling path of the Telemetry sensor, including the supported sampling path information
show telemetry dynamic-subscription [*dynamic-subscription-name*]	Display the Telemetry dynamic subscription statistics, including sensor path information of dynamic subscription.

11.13.3 Telemetry Typical Configuration Example

11.13.3.1 Configure Telemetry Static Subscription Function

Network Requirements

- Device acts as Telemetry client to actively deliver the data to the server.
- Enable the Telemetry service on the Server and actively monitors port 30000.

Network Topology

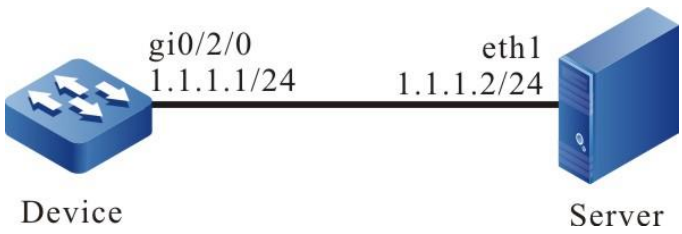


Figure 352 Networking of configuring Telemetry static subscription

Configuration Steps

Step 1: On Server, enable the Telemetry service, and monitor port 30000 (omitted).

Step 2: Configure Telemetry static subscription function.

#Create a sampling group sensor, and configure the sampling path as dmm/memInfo below to count data such as memory utilization.

```
Device#configure terminal
Device(config)#telemetry sensor-group sensor
Device(config-telemetry-sensor-group-sensor)#sensor-path dmm/memInfo
Device(config-telemetry-sensor-group-sensor)#exit
```

#Create a target group, configure the target address as the address of the server, and configure the port as the port monitored by Server.

```
Device(config)#telemetry destination-group dest
Device(config-telemetry-destination-group-dest)#ipv4-address 1.1.1.2 port 30000
Device(config-telemetry-destination-group-dest)#exit
```

#Configure the subscription group, reference the sensor combination target group configured above, and enable the subscription function.

```
Device(config)#telemetry subscription sub
Device(config-telemetry-subscription-sub)#sensor-group sensor sample-interval 10000
Device(config-telemetry-subscription-sub)#destination-group dest
Device(config-telemetry-subscription-sub)#subscription enable
```

Step 3: Check the result.

#The collector can receive the memory statistics sent by the device through Telemetry every 10s.

11.13.3.2 Configure Telemetry Dynamic Subscription Function

Network Requirements

- As a Telemetry client, Client is used to send a telemetry data request to the device and display the data replied by the device
- As a Telemetry server, Device is used to respond to device requests

Network Topology

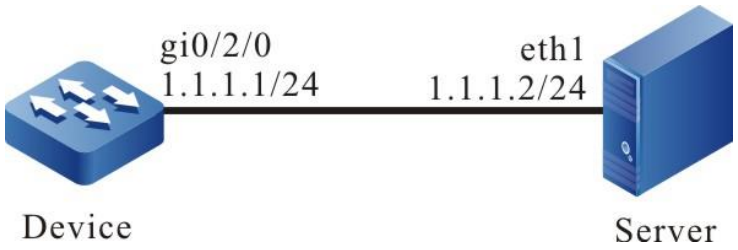


Figure 353 Networking of configuring Telemetry dynamic subscription

Configuration Steps

Step 1: Enable the GRPC service on the device.

```
Device#configure terminal
Device(config)#grpc server
```

Step 2: On Client, deliver the Telemetry data request (omitted).

Step 3: Check the result.

#On the device, show the dynamic subscription connection information.

```
Device#show telemetry dynamic-subscription

1.Telemetry dynamic-subscription Information:
 ------------------------------------------------------------------
 Subscription-name     : dynSubs96183
 Subscription-id       : 96183
 Request-id            : 3874318141
 Encoding              : JSON
 Sample-interval(ms):  : 10000
 Subscription-state:   : Subscribed
 ------------------------------------------------------------------
 Sensor group information:
 ------------------------------------------------------------------
 Sample-interval(ms)     Sample-path
 ------------------------------------------------------------------
 10000                   dmm/memInfo
 ------------------------------------------------------------------
```

12 Virtualization

12.1 VST

12.1.1 Overview

With the increasing requirement of the user for reducing the cost and improving the device reliability, Sofinet puts forward one technology of combining multiple physical switches to form one virtual switch, that is Virtual Switching Technology, called VST.

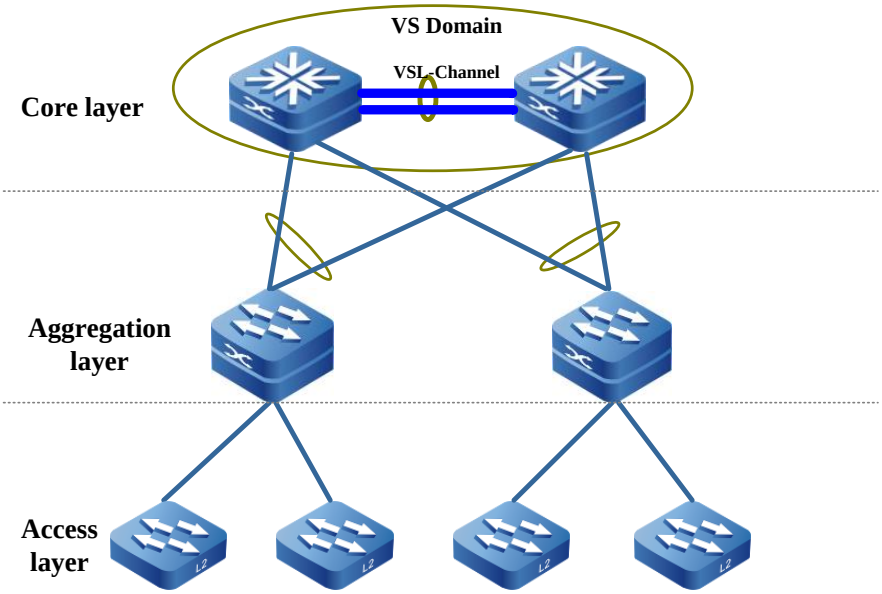


Figure 354 VST physical network view

As shown in figure 1-1, two devices of the core layer are connected via the VSL interface, forming one VS Domain (virtual switching domain, also called stacking system). The aggregation layer device is uplinked to VS Domain via the link aggregation. The VS Domain of the core layer is one virtual device for the other network devices.

Compared with the traditional L2 spanning tree and L3 VRRP/VBRP technology, the VST had the following advantages:

- The bandwidth increases multiplicatively and is used effectively

Because the traditional technology runs STP/RSTP/MSTP, one of the previous

two uplink links is in the forwarding state and the other is in the standby state. After using the VST, multiple devices become one logical device, so do not need to block some links. Two links form one aggregation group and both can be used to forward data, so as to make use of the bandwidth of the links efficiently, avoiding the waste of the bandwidth resources. Besides, the cross-device and cross-board aggregation link can provide the redundant links and also can realize the dynamic load balance, making use of all bandwidths efficiently.

- High reliability

The virtual switching system is formed by multiple member devices. The control device is responsible for the operation, management, and maintenance of the whole virtual switching system and the other member devices are in the standby sate. Once the control device fails and does not rely on the convergence of STP/RSTP/MSTP, VRRP/VBRP, the system elects one new control device from the standby member devices, ensuring that the services of the virtual switching system are not interrupted and improving the reliability when the member device fails.

- Simplify network topology

The virtual device formed by the VST is equivalent to one device in the network, connected with the around devices via the aggregation link. There is no L2 loop, so it is not necessary to configure the STP/RSTP/MSTP protocol. The control layer protocols run on one virtual device, reducing the exchanging of lots of protocol packets between devices and shortening the route convergence time.

- Unified management

After two or more devices form the stacking system, the control platform of the member devices in the virtual switching system are in the standby state, but the data platform is active. The user can log into the virtual switching system via the port of any member device and manages the whole virtual device in a unified manner, but does not need to connect to each member device for management.

12.1.2 Basic Concepts

Virtual Switching Domain

The virtual switching domain is formed by one or multiple member devices. The domain number configurations of the member devices in one virtual switching domain should be the same. The domain number uniquely determines one virtual switching domain. When the MAC address of the virtual switching domain uses the virtual MAC address mode to get, the number of the virtual switching domain uniquely decides the MAC address, so in one LAN, the domain numbers between multiple stacking systems cannot be the same.

Virtual Switching Member Device

Each physical device in the virtual switching domain is also called virtual switching member device. In one stacking domain, the member number uniquely determines one member device.

VSL Interface and Member Ports

Bind multiple physical ports with the stacking capability to form one virtual switching link channel (VSL-Channel). The VSL-Channel is the logical link channel of exchanging the protocol packets and forwarding service data between member devices. The physical port is called virtual switching link member port.

The member devices are added to one virtual switching domain and they are interconnected via the VSL-Channel, forming one virtual device.

LMP

LMP (Link Manage Protocol) is used to manage the VSL channel and the member ports.

RRP

RRP (Role Resolution Protocol) is used to elect the member device role in the

stacking system.

TDP

TDP (Topology Discovery Protocol) is used to advertise the member device information in the stacking system, ensuring the consistency of all member device information in the stacking system.

12.1.3 VST Function Configuration

Table 1555 VST function configuration list

Configuration Tasks	
Configure the virtual switching member device	Configure the virtual switching member device domain number
	Configure the virtual switching member device number
	Configure the virtual switching member device priority
Configure the VSL interface	Create one VSL interface
	Configure the port to add to the VSL interface
Configure the device running mode	Configure the device running mode
Configure the maximum devices supported by the stacking system	Configure the maximum devices supported by the stacking system

12.1.3.1 Configure Virtual Switching Member Device

Before the device is added to the virtual switching stacking domain or after being added to the virtual switching stacking domain, you can configure the device, including its member number, domain number, and priority.

Note

- In the VST mode, after modifying the member number or domain number of the virtual switching member device, the new configured member

number or domain number does not take effect at once, but takes effect only after the virtual switching member device saves the configuration and restarts.

Configuration Condition

None

Configure Domain Number of Virtual Switching Member Device

Table 1556 Configure the domain number of the virtual switching member device

Step	Command	Description
Enter the virtual switching member configuration mode	switch virtual member *member-id*	-
Configure the number of the virtual switching member device domain	domain *domain-id*	Mandatory By default, the number of the virtual switching member device is 100.

Caution

- In the VST mode, when adding the virtual switching member device to the virtual switching domain, ensure that the domain numbers of the virtual switching member devices are the same. Otherwise, the virtual switching member devices cannot be added to one virtual switching domain.
- In the VST mode, after modifying the domain number, the new domain number does not take effect at once, but takes effect only after the virtual switching member device saves the configuration and restarts.

Configure Virtual Switching Member Device Number

Configuring the number of the virtual switching member device includes two

cases:

1. The device is not ever configured with the number of the virtual switching member device and you need to configure one virtual switching member device number;
2. The device is configured with the number of the virtual switching member device and you need to modify to the new virtual switching member device number.

Therefore, there are two commands for configuring the number of the virtual switching member device: One is for configuring the number of the virtual switching member device and the other is for modifying the number of the virtual switching member device, as shown in Table 1-3.

Table 1557 Configure the VST member device number

Step	Command	Description
Enter the global mode	configure terminal	-
Configure the virtual switching member device number	switch virtual member *member-id*	Mandatory By default, the device does not have the virtual switching member device number.
Modify the virtual switching member device number	switch virtual member *member-id* rename *member-id-new*	Optional

Caution

- In the VST mode, after modifying the number of the virtual switching member device, save the configuration and restart the system so that the new virtual switching member device number can take effect.
- In one virtual switching domain, the member number of each virtual switching member device is unique. Otherwise, the virtual switching member device cannot stack normally.

Configure Virtual Switching Member Device Priority

When multiple virtual switching member devices are added to one virtual switching domain, you can configure the priority of the virtual switching member device to improve the possibility of the virtual switching member device being elected as the control device. The larger the priority value, the higher the possibility.

Table 1558 Configure the priority of the virtual switching member device

Step	Command	Description
Enter the virtual switching member configuration mode	switch virtual member *member-id*	-
Configure the priority of the virtual switching member device	priority *priority-num*	Mandatory By default, the priority of the virtual switching member device is 100.

Note

- The electing rule of the virtual switching control device in the virtual switching domain:
- The virtual switching control device is prior; when there are multiple virtual switching control devices, compare according to step 2. If there is no virtual switching control device, compare according to step 3. Otherwise, end the comparison.
- The virtual switching control device with longer running time is prior; if the running time is the same, compare according to step 3. Otherwise, end the comparison.
- The one with larger priority is prior. If the priority is the same, compare according to step 4. Otherwise, end the comparison.
- The one with the smaller member number is prior.

12.1.3.2 Configure VSL Channel

VSL-Channel is one logical interface and it binds multiple physical interfaces supporting stacking to manage the physical ports in a unified manner. Any operation for the VSL-Channel functions on each physical member port.

Configuration Condition

None

Create VSL Channel

Table 1559 Create VSL-Channel

Step	Command	Description
Enter the global mode	configure terminal	-
Create VSL-Channel	vsl-channel *vsl-channel-id*	Mandatory In the standalone mode, *vsl-channel-id* is one-dimension value, indicating the number of the virtual switching link interface; in the VST mode, it is the two-dimension value. The first dimension is the number of the virtual switching member and the second dimension is the number of the virtual switching link interface.

Caution

- When deleting the virtual switching link interface, all member ports in the VSL channel exit the VSL channel and all configurations of the member port restore to the default state. Before deleting the VSL channel, confirm that there is no loop in the network after deleting.

Configure Port to Add to VSL Channel

Table 1560 Configure a port to add to the VSL channel

Step	Command	Description
Enter the global mode	configure terminal	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure the port to add to the VSL channel	vsl-channel *vsl-channel-id* mode on	Mandatory

Note

- The port capability levels of all member ports in the VAL channel should be the same.
- If you need a non-original port rate for stacking, you need to manually configure the port rate.

12.1.3.3 Configure Device Running Mode

The current device supports two running modes, that is, standalone mode and stacking mode. The device can form one virtual switching domain with the other virtual switching member devices only when running in the VST mode.

Configuration Condition

None

Configure Device Running Mode

Table 1561 Configure the running mode of the device

Step	Command	Description
Enter the privileged user mode	enable	-
Configure the device running mode	switch mode { stand-alone | virtual }	Mandatory By default, the device runs in the standalone mode.

Note

- After the running mode of the device changes, the device restarts and runs by the new configuration mode after restarting.
- Different running modes of the devices correspond to their own independent startup configuration files.
- Before the device switches to run in the VST mode, ensure that the virtual switching member device number is configured. Otherwise, it cannot switch.

12.1.3.4 VST Monitoring and Maintaining

Table 1562 VST monitoring and maintaining

Command	Description
show switch virtual	Display the basic information of the virtual switching domain
show switch virtual local config	Display the basic configuration information of the local virtual switching member device
show switch virtual local current	Display the basic running information of the local virtual switching member device
show switch virtual member *member-id* [config | current]	Display the basic information of the virtual switching member device
show switch virtual topo	Display the forwarding path information of the local virtual switching member device to the other virtual switching member devices in the virtual switching domain
show switch vsl-channel [*vsl-channel-id*]	Display the information of the VSL channel in the virtual switching domain

12.1.4 VST Typical Configuration Example

12.1.4.1 Configure Devices to Form Link Stacking System

Network Requirement

- Device0, and Device1 form the link stacking system; Device0 becomes the control device.

Network Topology

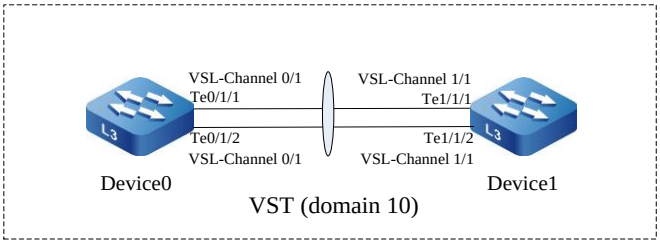


Figure 355 Configure devices to form the link stacking system

Configuration Steps

Step 1 Configure Device0.

#On Device0, configure the virtual switching member device number as 0, configure the domain number as 10, and the priority is 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 virtual switch link interface 1 and add port tengigabitethernet1/1 and tengigabitethernet1/2 to the virtual switch 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
```

#Save the configuration on Device0.

```
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 the virtual switching member device number as 1, configure the domain number as 10, and the priority is 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 virtual switch link interface 1 and add port tengigabitethernet0/1 and tengigabitethernet0/2 to the virtual switch link interface 1.

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 0/1-0/2
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 the running mode of Device0 and Device1 as the VST

mode.

#Configure the running mode of Device0 as the VST 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 the running mode of Device1 as the VST 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.

#On Device0, the VST system is formed and Device0 is the master device.

```
Device0#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode       : VIRTUAL
Virtual Switch DomainId   : 10
Virtual Switch mac-address : 0101.7a6a.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
```

12.2 MAD

12.2.1 Overview

When the VSL channel in the stacking system fails, the stacking system is split to multiple virtual switching domains and there are multiple virtual switching control devices with the same global configuration (called control device for short). This is called multi-active. The global configuration of the split logical device is the same as that of the previous logical device, so there is network configuration conflict, resulting in the traffic abnormality. To avoid the influence for the services, MAD (Multi-Active Detection) emerges.

The current stacking system supports two MAD modes: MAD LACP, and MAD Fast-Hello, meeting different networking requirements.

The MAD status includes two kinds: Active and Recovery. Active indicates the normal working state and Recovery indicates the disabling state. In the Recovery state, all L2/L3 Ethernet interfaces and VLAN interfaces except for the VSL member ports and reserved ports are disabled by MAD.

When the device receives the MAD detection packets, compare the data in the packet with the data of the local logical device. If the VS Domain ID in the packet (virtual switching domain number of the sending end) is the same as that of the local logical device, and the Master ID in the packet (the member number of the control device in the virtual switching domain of the sending end) is different from the local logical device, it is regarded that multi-active happens and start the multi-active election. According to some election rules, in one virtual switching domain, just reserve one logical device to keep Active and the other logical devices enter the Recovery state.

During the MAD LACP networking, use the intermediate device; during the MAD Fast-Hello networking, you can use the intermediate device and also can adopt the direct-connection. If adopting the direct-connection mode, you need to ensure that there is the direct-connection line between any two virtual switching member devices for the MAD, that is, it is necessary to ensure the full connection.

12.2.2 MAD Function Configuration

Table 1563 MAD function configuration list

Configuration Tasks	
Configure MAD LACP function	Configure MAD LACP function
Configure MAD Fast-Hello function	Configure MAD Fast-Hello function
Configure the reserved port	Configure the reserved port
Configure restoring the MAD status to Active	Configure restoring the MAD status to Active

12.2.2.1 Configure MAD LACP Function

MAD LACP realizes the multi-active detection and election by expanding the LACP protocol packet field.

Configuration Condition

None

Configure MAD LACP Function

Table 1564 Configure the MAD LACP function

Step	Command	Description
Enter the global mode	configure terminal	-
Create one dynamic aggregation group	link-aggregation *link-aggregation-id* mode lacp	Mandatory By default, do not create the specified aggregation group.
Enter the aggregation group configuration mode	interface link-aggregation *link-aggregation-id*	-
Enable the MAD LACP function	mad enable	Mandatory By default, do not enable the MAD LACP function.

Note

- Dynamic aggregation group supports enabling the MAC LACP function.

- The intermediate device used by networking should be Sofinet device that supports the LACP packet transparent transmission function.

12.2.2.2 Configure MAD BFD Function

MAD BFD multi-activation detection realizes multi-activation detection and election by expanding the packet field of the BFD protocol.

Configuration Condition

None

Configure MAD BFD Function

Table 1565 Configure the MAD BFD function

Step	Command	Description
Enter the global mode	configure terminal	-
Enter the interface configuration mode	interface dc 0/1	-
Configure MAD IP address	mad member *member-id* ip address *ip-address network-mask*	-
Enable the MAD BFD function	mad bfd enable	Mandatory By default, the interface does not enable the MAD BFD function.

Note

- It is recommended to match the MAD IP address corresponding to all member numbers to prevent modifying the member number of a device, but the MAD IP address corresponding to the new member number is not configured, resulting in the ineffective MAD BFD function.

- The virtual switching member device used in networking must support BFD function.
- After the MAD BFD is enabled, if the DC port is configured as a reserved port, please ensure that the MAC address of the DC port is the default address of the system, so as to avoid MAC address conflict in the network after multiple activation.

12.2.2.3 Configure MAD Fast-Hello Function

The protocol packets of MAD Fast-Hello are defined by Sofinet and directly carry the data needed by the MAD and election.

Configuration Condition

None

Configure MAD Fast-Hello Function

Table 1566 Configure the MAD Fast-Hello function

Step	Command	Description
Enter the global mode	configure terminal	-
Configure the sending period of the MAD Fast-Hello packets in the normal mode	mad fast-hello normal interval *interval-time*	Optional By default, the sending period of the MAD Fast-Hello packets in the normal mode is 2000ms.
Configure the sending period of the MAD Fast-Hello packets in the aggressive mode	mad fast-hello aggressive interval *interval-time*	Optional By default, the sending period of the MAD Fast-Hello packets in the aggressive mode is 500ms.
Configure the direction of the aggressive mode	mad fast-hello aggressive duration *duration-time*	Optional By default, the duration of the aggressive mode is 120s.
Enter the VLAN configuration mode	vlan *vlan-id*	-

Step	Command	Description
Configure the control VLAN	mad fast-hello control-vlan	Mandatory By default, do not configure the control VLAN.
Enter the global mode	exit	-
Enter the L2 Ethernet interface configuration mode	interface *interface-name*	-
Configure the link type of the port as Trunk	switchport mode trunk	Mandatory By default, the port link type is Access.
Disable the spanning tree function of the port	no spanning-tree enable	Mandatory By default, the port enables the spanning tree function.
Configure the control port	mad fast-hello vlan *vlan-id*	Mandatory By default, do not configure the control port.

Note

- The control VLAN and control port of MAD Fast-Hello can only be used for MAD Fast-Hello and cannot configure other services any more.
- On the control port of MAD Fast-Hello, disable the spanning tree function of the port.

12.2.2.4 Configure Reserved Port

When the MAD status changes to Recovery, the reserved port is not disabled by MAD and you can configure the port, interface (console port) that have the special usage and need to keep UP as the reserved port.

Configuration Condition

None

Configure Reserved Port

Table 1567 Configure the reserved port

Step	Command	Description
Enter the global mode	configure terminal	-
Enter the L2/L3 Ethernet interface configuration mode	interface *interface-name*	Either After entering the L2/L3 Ethernet interface configuration mode, the subsequent configuration takes effect only on the current interface; after entering the aggregation group configuration mode, the subsequent configuration takes effect only on the aggregation group; after entering the interface configuration mode, the subsequent configuration just takes effect on the current interface.
Enter the aggregation group configuration mode	link-aggregation *link-aggregation-id*	
Enter the interface configuration mode	interface vlan *vlan-id*	
Configure the reserved port	mad exclude recovery	Mandatory By default, do not configure the reserved port.

Note

- The aggregation group enabled with the MAD LACP function cannot be configured as the reserved port.

12.2.2.5 Configure Recovering MAD Status to Active

Configuration Condition

None

Configure Recovering MAD Status to Active

Table 1568 Configure recovering the MAD status to Active

Step	Command	Description
Enter the global mode	configure terminal	-
Configure recovering the MAD status to Active	mad restore	Mandatory By default, the MAD status changes to Active.

Note

- When the MAD status changes to Recovery, for the disabled port and interface, MAD does not process. When the MAD status changes to Active, just enable the port and interface disabled by MAD.

12.2.2.6 MAD Monitoring and Maintaining

Table 1569MAD monitoring and maintaining

Command	Description
show mad exclude recovery interface [switchport | vlan]	Display the configured reserved port
show mad fast-hello	Display the MAD Fast-Hello information
show mad lacp	Display the MAD LACP information
show mad status	Display the MAD status

12.2.3 MAD Typical Configuration Example

12.2.3.1 Configure MAD LACP Function

Network Requirements

- Device0 and Device1 form the stacking system with Device0 as the control device. PC1 accesses IP Network via the stacking system.
- Configure the MAD LACP function so that PC1 can access IP Network

normally after Device1 is split from the stacking system because of the VSL channel failure and the services do not become abnormal because of the network configuration conflict.

Network Topology

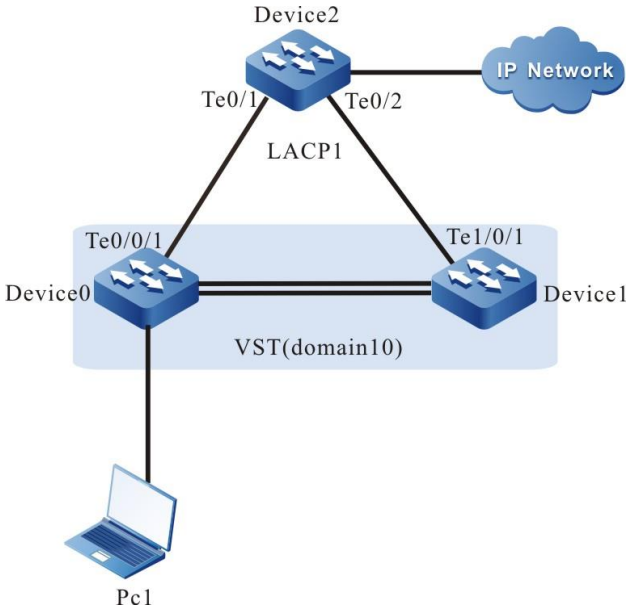


Figure 356 Networking of configuring the MAD LACP function

Configuration Steps

Step 1: Make Device0 and Device1 form the stacking system with Device0 as the control device. (Omitted)

Step 2: Configure the MAD LACP function on Device0.

#Create VLAN2 on Device0, create dynamic aggregation group 1, configure the link type of the aggregation group 1 as Trunk, and permit the services of VLAN2 to pass.

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#exit
Device0(config)#link-aggregation 1 mode lacp
Device0(config)#interface 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 group 1.

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#link-aggregation 1 active
Device0(config-if-range)#exit
```

#Enable the MAD LACP function on aggregation group 1 of Device0.

```
Device0(config)#interface link-aggregation 1
Device0(config-link-aggregation1)#mad enable
Device0(config-link-aggregation1)#exit
```

Step 3: Configure Device2.

#On Device2, create VLAN2 and configure the link type of port tengigabitethernet0/1, tengigabitethernet0/2, permitting the services of VLAN2 to pass.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#link-aggregation 1 mode lacp
Device2(config)#interface 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, disable the spanning tree function of port tengigabitethernet0/1,tengigabitethernet0/2.

```
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.

#View the MAD LACP information on Device0.

```
Device0#show mad lacp
------------MAD-LACP INFORMATION--------------
  Link-aggregation      Mad state
 -----------------      -----------------
      1            enable
```

#After Device1 is split from the stacking system because of the VSL channel failure, the MAD status of the stacking system with Device0 as the control device is Active, and the MAD status of the stacking system with Device1 as the control device is Recovery.

```
Device0#show mad status
 MAD status: active
auto-restore: disable
auto-restore detect interval: 3 min

Device1#show mad status
 MAD status: recovery
auto-restore: disable
auto-restore detect interval: 3 min
```

#PC1 can access IP Network.

12.2.3.2 Configure MAD BFD Function

Network Requirements

- Device0 and Device1 form the stacking system with Device0 as the control device.
- Configure the MAD BFD function so that after Device1 is separated from the stacking system due to virtual switching link interface failure, there will be no service abnormalities caused by network configuration conflict.

Network Topology

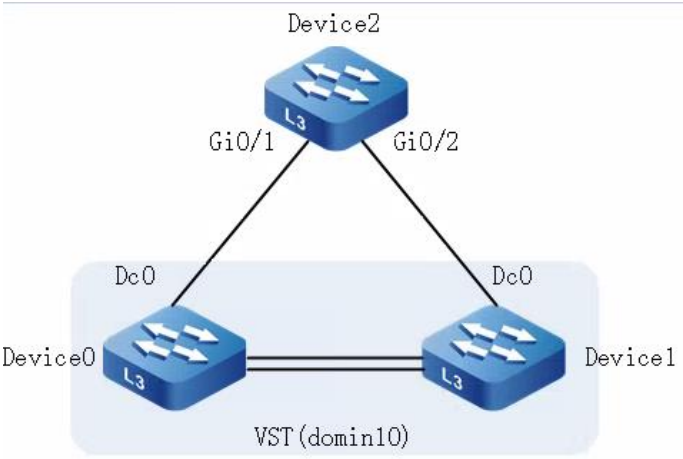


Figure 357 Networking of configuring MAD BFD

Configuration Steps

Step 1: Device0 and Device1 form the stack system with Device0 as the control device.

Step 2: On Device0, configure the MAD BFD function.

#On DC0 interface of Device0, enable the MAD BFD function and configure the MAD IP addresses of the corresponding devices of all member numbers.

```
Device0(config)#interface dc 0
Device0(config-if-dc0)#mad bfd enable
Device0(config-if-dc0)#mad member 0 ip address 192.168.1.1 255.255.0.0
Device0(config-if-dc0)#mad member 1 ip address 192.168.1.2 255.255.0.0
Device0(config-if-dc0)#exit
```

Step 3: Configure Device2.

#On Device2, create VLAN2, and add the ports gigabitethernet0/1 and gigabitethernet0/2 to VLAN2. (omitted)

Step 4: Check the result.

#On Device0, view the enabling information of MAD BFD.

```
Device0#show mad bfd
----------------MAD-BFD INFORMATION----------------
----------  --------------- ------------ ---------
 Interface   ActiveIP       Mad state    MasterID
----------  --------------- ------------ ---------
 dc0        129.255.1.1     enable       0

   memberID    IP address      mask address
   --------    --------------- -------------
   0           192.168.1.1     255.255.0.0
   1           192.168.1.2     255.255.0.0
```

#When Device1 is separated from the stacking system due to virtual switching link interface failure, the MAD state of the stacking system with Device0 as the main

control device is Active, and the MAD state of the stacking system with Device1 as the main control device is Recovery.

```
Device0#show mad status
 MAD status: active
auto-restore: disable
auto-restore detect interval: 3 min
Device1#show mad status
 MAD status: recovery
auto-restore: disable
auto-restore detect interval: 3 min
```

12.2.3.3 Configure MAD Fast-Hello Function

Network Requirements

- Device0 and Device1 form the stacking system with Device0 as the control device.
- Configure the MAD Fast-Hello function so that the services do not become abnormal because of the network configuration conflict after Device1 is split from the stacking system because of the VSL channel failure.

Network Topology

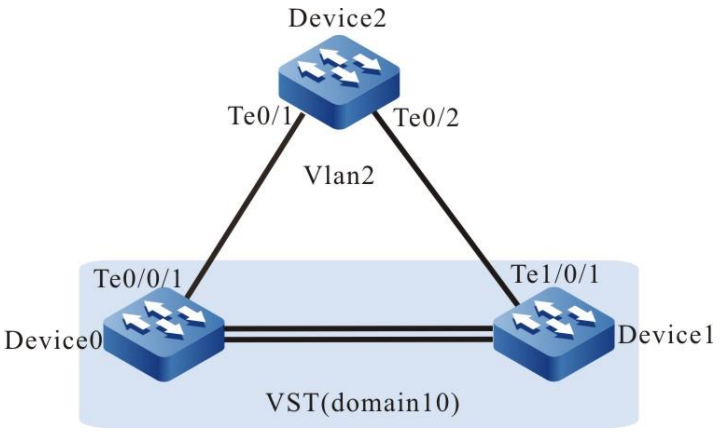


Figure 358 Networking of configuring the MAD Fast-Hello

Configuration Steps

Step 1: Make Device0 and Device1 form the stacking system with Device0

as the control device. (Omitted)

Step 2: Configure the MAD Fast-Hello function on Device0.

#Create VLAN2 on Device0 and configure as the control VLAN of MAD Fast-Hello.

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#mad fast-hello control-vlan
Device0(config-vlan2)#exit
```

#On Device0, configure the link type of port gigabitethernet0/0/1,gigabitethernet1/0/1 as Trunk and add to the control VLAN of MAD Fast-Hello.

```
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
```

#Disable the spanning tree function of the port gigabitethernet0/0/1, gigabitethernet1/0/1on Device0.

```
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.

#Create VLAN2 on Device2, configure the link type of the port gigabitethernet0/1,gigabitethernet0/2 as Trunk, and permit the services of VLAN2 to pass.

```
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
```

#Disable the spanning tree function of the port gigabitethernet0/1,gigabitethernet0/2 on Device2.

```
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.

#View the MAD Fast-Hello enabling on Device0.

```
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
```

#After Device1 is split from the stacking system because of the VSL channel failure, the MAD status of the stacking system with Device0 as the control device is Active, and the MAD status of the stacking system with Device1 as the control device is Recovery.

```
Device0#show mad status
 MAD status: active
auto-restore: disable
auto-restore detect interval: 3 min
Device1# show mad status
 MAD status: recovery
auto-restore: disable
auto-restore detect interval: 3 min
```

12.3 MVST

12.3.1 Overview

At present, the VST (virtual switching technologies, which combines several horizontal physical devices into a virtual device) technology has gradually become a necessary networking technology for LAN because of its high reliability and easy management. The VST technology realizes the unified management of multiple devices at the same level, but there is still the problem of decentralized management of

devices in multi-level network. Especially in the typical two-layer LAN, the access layer uses a large number of access devices, which are large in number and strong in dispersion, and need to be maintained and managed one by one. The management is very cumbersome. In addition, assigning an IP address to these devices will consume a lot of IP address resources, which is undoubtedly a waste under the current shortage of IP address resources.

To solve the above problems, the MVST (mix virtual switching technology) technology is proposed. As shown in the figure below, the core layer of LAN adopts the VST technology to virtualize multiple devices into one logical device, while the MVST (mix virtual switching technology) technology is used vertically, which makes all devices in the LAN virtual as one logical device, forming a unified management domain (MVST domain). The management domain provides a management IP address to the outside, and provides the management and access ability for each device in the LAN. It really realizes "one network, one machine", one network, one IP, and one device can easily manage the whole LAN, greatly simplifying the management.

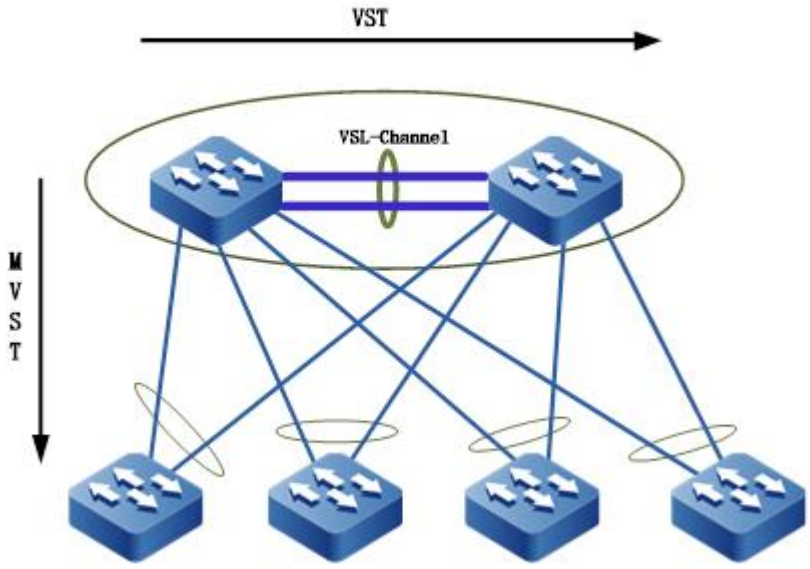


Figure 359 MVST physical network view

According to the location and function of the device in the LAN, MVST defines three device roles:

- Master device (MVST master): Responsible for configuring, managing and monitoring all devices in the LAN.
- Extended card (MVST Slave slot): The extended card in the LAN, accepting the unified configuration and management of the master device.
- Candidate card (MVST Candidate): It is not added to the MVST domain, but has the conditions of becoming the extended card.

The master device in the MVST domain discovers the extended card via the MVST detection protocol, collects the information of each extended card in the MVST domain via the MVST topology collection protocol, and draws the LAN topology view. The master device adds the access device to the MVST domain according to the topology view.

After the extended card is added to the MVST domain, the user can log into the control interface of the master device via the IP address of the master device, realizing the unified management for the whole LAN. Besides the general configuration and management, the MVST technology provides the following functions:

1. Template configuration

In the application scenario, if some configuration belongs to the public basic configuration and all extended cards in the MVST domain need to apply the configuration, you can edit the configuration to the configuration template and the master device delivers the configuration template to the extended card, which completes the public basic configuration.

2. Auto configuration

The master device backs up the startup configuration file of the extended card to the local storage media. When the extended card fails and needs to be replaced with one new extended card, the new extended card does not need any configuration, but directly accesses the LAN via one interface and the master device automatically delivers the backup configuration file to the extended card. In this way, the extended card completes the configuration and the network recovers fast.

3. One-key configuration

The master device can enable the Dot1x, storm control, DHCP Snooping, and Arp-check functions of all extended cards in the MVST domain by one key.

4. Auto upgrade

The master device prepares the SOFOS of the extended card in advance. When the extended card is added to the MVST domain, the master device automatically detects whether the running version of the extended card is consistent with the auto upgrade version. If not consistent, the background executes the auto upgrade. On the visible interface of the user, print the log information. When the extended card upgrades, the user still can manage the master device or extended card.

5. Password dynamic management

In the MVST domain, the login passwords of all extended cards are generated by the master device dynamically. After the extended card is added to the MVST domain successfully, the master device generates the dynamic password and delivers the password to the extended card. If the extended card needs to log in via console directly during running, the login password can only be got by the master device, strengthening the LAN security.

12.3.2 MVST Function Configuration

Table 1570 MVST function configuration list

Configuration Task	
Configure MVST basic functions	Configure the master device
	Configure the extended card
Configure MVST parameters	Configure the interval of sending the detection packet
	Configure the age time of the neighbor
	Configure the keepalive interval of the extended card
	Configure the connection status timeout of the extended card

Configuration Task	
	Configure the topology parameters
Configure the MVST feature functions	Configure the upgrade function
	Configure the profile function
	Configure the auto binding configuration function
	Configure the individual configuration
	Configure the device group function
	Configure the log function

12.3.2.1 Configure MVST Basic Functions

When hoping to manage the devices in one domain via the MVST technology, the user can configure MVST. In the MVST configuration tasks, first enable the MVST function so that the other function configuration can take effect.

Configuration Condition

None

Configure Master Device

The master device is the nerve center of MVST. It provides one management channel for the MVST domain. The administrator manages the devices of the specified domain in a unified manner via the channel.

Table 1571 Configure the master device

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the MVST function	mvst enable	Mandatory By default, the MVST function is disabled.
Configure the specified device as the master device of the MVST domain	mvst master	Mandatory By default, do not specify the master device.

Step	Command	Description
Configure the MVST domain name	mvst domain-name *domain-name*	Optional By default, the MVST domain name is mvst-1.
Create the MVST private aggregation port	mvst link-aggregation	Create the MVST link aggregation port
Add the members of the aggregation group	mvst interface *interface-name join* link-aggregation *link-aggregation-id* active	Add a member port to the MVST aggregation group
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	interface link-aggregation *link-aggregation-id*	
Enable the MVST detection on the port	mvst inspection	Mandatory By default, the MVST detection function of the port is disabled.

Configure Extended Card

When hoping to manage one device via MVST, the user can configure the device as the extended card of the MVST domain. The box device enables the MVST function, enabling the MVST detection function on the port or link aggregation.

Table 1572 Configure the extended card

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enable the MVST function	mvst enable	Mandatory

Step	Command	Description
		By default, the MVST function is disabled.
Enter the L2 Ethernet interface configuration mode	interface interface-name	Either After entering the L2 Ethernet interface configuration mode, subsequent configurations will only take effect on the current port; After entering the aggregation group configuration mode, subsequent configurations will only take effect in the aggregation group.
Enter the aggregation group configuration mode	Interface link-aggregation link-aggregation-id	
Configure the downlink port to enable the MVST detection	mvst inspection	Mandatory By default, the MVST detection function of the port is disabled.

12.3.2.2 Configure MVST Parameters

Configuration Condition

Before configuring the MVST parameters, first complete the following task:

- Configure the master device

Configure the Interval of Sending the Detection Packet

The device enabled with the MVST function periodically sends the detection packet to discover the connected device and extract the key information from the detection packet to form its own neighbor device information table.

Table 1573 Configure the interval of sending the detection packet

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the interval of sending the MVST detection packet	mvst inspection timer *timer-value*	Mandatory By default, the interval of sending the MVST detection packet is 10s.

Configure the Age Time of the Neighbor

The age time of the neighbor indicates the life time of the local device information on the neighbor device so that the neighbor device can delete the local device information after the life time of the local device arrives.

Table 1574 Configure the age time of the neighbor

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the age time of the local device information in the neighbor device	mvst inspection aging-time *aging-time-value*	Mandatory By default, the age time of the local device information in the neighbor device is 30s.

Configure the Keepalive Interval of the Extended Card

After the extended card is added to the MVST domain, the master device and extended card start to exchange the keepalive packets. By default, the keepalive packet is exchanged every 8s. If the master device does not receive three keepalive packets of the extended card successively, change the Active status of the extended card to the Connect status.

Table 1575 Configure the keepalive interval of the extended card

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the keepalive	mvst handtime *handtime-value*	Mandatory

Step	Command	Description
interval of the extended card		By default, the keepalive interval of the extended card is 8s.

Configure Connect Status Timeout of Extended Card

If the master device receives the keepalive packet sent by the extended card within the valid time of the connect status, change the Connect status of the extended card to the Active status. If not receiving the keepalive packet sent by the extended card, change the Connect status of the extended card to the Disconnect status.

The master device does not send the keepalive packet to the extended card in the Disconnect status any more until receiving the keepalive packet sent by the extended card again.

Table 1576 Configure the connect status timeout of the extended card

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the Connect status timeout of the extended card	mvst holdtime *holdtime-value*	Mandatory By default, the Connect status timeout of the extended card is 80s.

Configure Topology Parameters

After the MVST domain is set up, the master device regularly collects the topology information of the whole MVST domain via the topology request packet. When the topology request packet is spreading in the network, lots of network devices will receive the topology request packet at the same time, and send the topology response packet, which may cause the network block. To reduce the phenomenon, the second port starts to forward the topology request packet after the master device waits for the delay time of each port forwarding the topology collection request packet…..until the last port completes the forwarding of the topology request packet.

Table 1577 Configure the topology parameters

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the topology collection period	mvst topo hello-time *hello-time-value*	Mandatory By default, the topology collection period is 30s.
Configure the delay time of the master device port collecting the topology	mvst topo port-delay-time *port-delay-time-value*	Optional By default, the delay time of the master device port collecting the topology is 100ms.

12.3.2.3 Configure MVST Functions

Configuration Condition

Before configuring MVST functions, first complete the following task:

- Configure the MVST basic functions

Configure the Upgrade Function

The upgrade function indicates that the master device upgrades the system mirror file or Monitor file of the extended card.

There are two modes of upgrading the system mirror file or Bootloader file of the extended card:

1. Auto upgrade: After the extended card is added to the MVST domain successfully, the master device automatically detects whether the running version of the extended card is consistent with the auto upgrade version. If not consistent, upgrade the extended card automatically.
2. Manual upgrade: The user upgrade the system mirror file or Bootloader file of the extended card in real time via the command line

mode according to the real-time demand.

Table 1578 Configure the upgrade function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the auto upgrade	mvst auto update image { *path/image-name* | *image-name* } [*ip-address* { ftp *user-name user-password* | tftp } [reload [write]]	Mandatory By default, no auto upgrade configuration.
Enter the privileged user mode	exit	-
Configure upgrading the extended card manually	mvst update slave-slot *slave-slot-id* { image | bootloader } { *path/filename* | *filename* } [*ip-address* { ftp *user-name user-password* | tftp } [reload] | reload] or mvst update device-group *device-group-id* { image | bootloader } { *path/filename* | *filename* } [*ip-address* { ftp *user-name user-password* | tftp } [reload] | reload]	Optional

Note

- Before configuring the auto upgrade, it is necessary to ensure that the version file already exists.

Configure the Template Function

The template function can complete the batch configuration and management, which is convenient for the network maintenance. The user edits the public basic configuration to one txt file according to the network operation and maintenance

requirement, and then, the master device delivers the file to the extended card. The extended card completes the public basic configuration.

Table 1579 Configure the template function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Specify the configuration template	mvst configure template *template-name*	Mandatory By default, do not specify the configuration template.
Configure the master device to deliver the configuration template to the extended card	mvst apply configure template {service-group *service-group-id* | slave-slot { *slave-slot-id* | all } }	Optional

Note

- After the master device delivers the configuration template to the extended card, execute the **write slave-slot** or **write device-group** command to make all extended cards save the configuration information to the startup configuration file.

Configure Auto Binding Configuration Function

The master device backs up the startup configuration file of all extended cards in the MVST domain to the local storage media via the auto binding configuration. When the extended card needs to change because of fault and other reasons, the new extended card can completes the configuration automatically via the backup startup configuration file.

Table 1580 Configure the auto binding configuration function

Step	Command	Description
Enter the global configuration mode	configure terminal	-

Step	Command	Description
Configure the port to bind with the startup configuration file	mvst bind startup interface {*interface-list* | link-aggregation *link-aggregation-id*} | all	Mandatory By default, the port is not bound with the startup configuration file.

Configure Individual Configuration

The extended cards in the MVST domain will bear different network services because of the network environment, so the configuration of the extended card needs to be individual. The administrator can log into the virtual configuration interface of the extended card via the master device and complete the configuration management of the extended card.

Table 1581 Configure the individual configuration

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the extended card	configure slave-slot *slave-slot-id*	Mandatory Log into the virtual configuration interface of the extended card
Enter the privileged user mode	exit	-
Configure the extended card to save the current configuration information to the startup configuration file	write slave-slot *slave-slot-id*	Optional

Configure Device Group Function

When all extended cards in the device group need to realize the same function, you can configure the device group to realize the batch configuration management. The administrator can log into the virtual configuration interface of the configuration sample of the device group via the master device, and complete the configuration management of the device group.

Table 1582 Configure the device group function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the device group	configure device-group *device-group-id* slave-slot *slave-slot-id*	Mandatory The administrator logs into the virtual configuration interface of the configuration sample of the device group.
Enter the privileged user mode	exit	-
Configure all extended cards in the device group to save the current configuration information in the startup configuration file	write device-group { *device-group-id* | all }	Optional

Configure the Service Group Function

When all extended cards in the service group need to achieve the same function, the batch configuration management can be completed by configuring the service group, such as configuring the same configuration template. The administrator can log in to the service group interface through the management device to manage the configuration of the service group.

Table 1583 Configure the service group function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the service group	mvst service-group *service-group-id*	Mandatory Create and enter the service group
Add a member	In the service configuration mode slave-slot *slave-slot-id*	Mandatory Add the extended card to the service group
Specify the configuration	configure template */flash/filepath*	Optional

Step	Command	Description
template of the service group		Specify all extended cards in the service group to execute the same configuration template
Enter the privileged user mode	exit	-

Configure the Log Function

The MVST log function indicates that the extended card sends the log information of the local device to the master device. The administrator can modify the log level rang sent by the extended card to the master device according to the network environment requirement.

Table 1584 Configure the log function

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the log level sent by the extended card to the master device	mvst slave-slot logging [*logging-level1 logging-level2*]	Mandatory By default, the log level sent by the extended card to the master device is 0-5.

12.3.2.4 MVST Monitoring and Maintaining

Table 1585 MVST monitoring and maintaining

Command	Description
show mvst auto-update config	Display the auto upgrade configuration information
show mvst device-group [*device-group-id*]	Display the configuration executing information of the specified device group
show mvst servcie-group [*servcie -group-id*]	Display the service group and specify the service group information
show mvst inspection	Display the neighbor information of the device

Command	Description
show mvst inspection opened	Display the port enabled with the MVST detection function
show mvst inspection queue	Display the MVST detection queue information
show mvst slave-slot	Display the information of the extended card in the MVST domain
show mvst slave-slot *slave-slot-id* command	Display some key running information of the specified extended card
show mvst slave-slot logging	Display the log level rang sent by the extended card to the master
show mvst slave-slot password	Display the login password table of the extended card
show mvst slave-slot { *slave-slot-id* use–info | use-info }	Display the using information of the extended card number
show mvst startup bind info	Display the port binding information
show mvst statistics	Display the statistics information of the sent and received MVST packets
show mvst summary	Display the abstract information of the MVST domain
show mvst topo config	Display the configuration information of the topology parameters
show mvst topo information [slave-slot *slave-slot-id*]	Display the topology information
show mvst tunnel	Display the channel information between the master device and extended card in the MVST domain
show mvst upgrade-information { device-group *device-group-id* | slave-slot { all | *slave-slot-id* } }	Display the upgrade status information of the extended card
show mvst write-information device-group { { *device-group-id* | all } | slave-slot *slave-slot-id* }	Display the status information of the extended card saving the current configuration
show running-config slave-slot *slave-slot-id*	Display the current configuration information of the extended card
show startup-config slave-slot *slave-slot-id*	Display the startup configuration file content of

Command	Description
	the extended card

12.3.3 MVST Typical Configuration Example

12.3.3.1 Configure Auto Detection Upgrade

Network Requirement

- Device1 and Device2 form the stacking system and serve as the MVST master device; Device3, Device4, and Device5 serve as the extended card and the last ports of the extended card are connected to the MVST master device.
- The master device configures the auto detection upgrade. When Device3, Device4, and Device5 are added to the MVST domain as the extended card, the extended card can upgrade automatically.

Network Topology

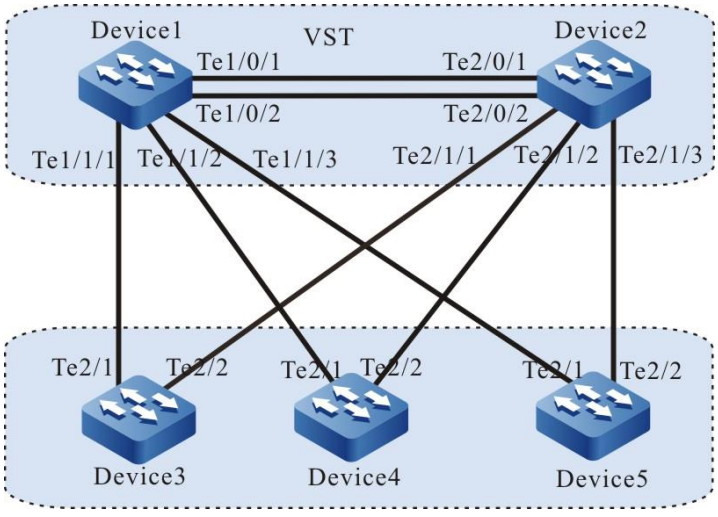


Figure 360 Configure the auto detection upgrade

Configuration Steps

Step 1: Configure the VST system.

#On Device1, configure the virtual switch member device No. to 1, and the domain No. to 10, and the priority to 255.

```
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 255
Device1(config-vst-member-1)#exit
```

#On Device1, create virtual switch link interface 1, and add ports tentengigabitethernet0/1 and tentengigabitethernet0/2 to virtual switch link interface 1.

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tentengigabitethernet 0/1
Device1(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/1)#exit
Device1(config)#interface tentengigabitethernet 0/2
Device1(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/2)#exit
```

#On Device 1, 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
```

#On Device2, configure the virtual switch member device No. to 2, and the domain No. to 10, and the priority to 200.

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
Device2(config-vst-member-2)#exit
```

#On Device2, create virtual switch link interface 1, and add port tentengigabitethernet1/1to virtual switch link interface 1.

```
Device2(config)#vsl-channel 1
```

```
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tentengigabitethernet 0/1
Device2(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/1)#exit
Device2(config)#interface tentengigabitethernet 0/2
Device2(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/2)#exit
```

#On Device2, save the configuration.

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

#Configure Device1 running mode to the 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!
%SYS-5-RELOAD: Reload requested
```

#Configure the running mode of Device2 to the stacking mode.

```
Device2#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!
%SYS-5-RELOAD: Reload requested
```

#After restarting, view on Device1, the stacking system is formed, and Device1 is the master device of the stacking system.

```
Device1#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode       : VIRTUAL
```

```
Virtual Switch DomainId    : 10
Virtual Switch mac-address : 0101.7a6a.0255

--------------- VST MEMBER INFORMATION -----------------
CODE MemberID Role   Pri  LocalVsl      RemoteVsl
--------------------------------------------------------------------------------
L   1      Master 255  vsl-channel 1/1   vsl-channel 2/1
    2      Member 200  vsl-channel 2/1   vsl-channel 1/1
```

Step 2: Configure the MVST basic functions.

#On Device1, configure the stacking system as the MVST management device.

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

#On Device1, configure the link aggregation of the stacking system, and enable the MVST detection.

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

#On Device3, enable the MVST function.

```
Device3#configure terminal
Device3#configure terminal
Device3(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit
```

```
%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.
```

#On Device4, enable the MVST function.

```
Device4#configure terminal
Device4(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device4(config)#mvst link-aggregation 2 mode lacp
Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active
Device4(config)#interface link-aggregation 2
Device4(config-link-aggregation2)#mvst inspection
Device4(config-link-aggregation2)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.
```

#On Device5, enable the MVST function.

```
Device5#configure terminal
Device5(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device5(config)#mvst link-aggregation 3 mode lacp
Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active
Device5(config)#interface link-aggregation 3
Device5(config-link-aggregation3)#mvst inspection
Device5(config-link-aggregation3)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.
```

Step 3: Configure auto upgrade detection.

#On Device1, configure auto upgrade detection, specify the upgrade version of the extended card, and add the clear, reload, and write parameters.

```
Device1(config)# mvst auto update image /flash/sp26-g-9.6.0.1(R).pck reload write
```

#On Device1, check the configuration result.

```
Device1(config)# show mvst auto-update config
------------------------------------------------------------------------------------------------------------
OPTION Codes:
  R -- Reload slave slot when update slave slot successfully
  W -- Save slave slot current configuration to startup-config
------------------------------------------------------------------------------------------------------------

------------------------------------------------------------------------------------------
```

```
--------------------------
ID   OPTION   IMAGE-NAME                    IMAGE-PATH
-------------------------------------------------------------------------------
--------------------------
1    None     sp25-g-9.6.1.1(R).pck          /flash/sp25-g-9.6.1.1(R).pck
2    R        sp23-g-9.6.1.1(R).pck         /flash/sp23-g-9.6.1.1(R).pck
3    RW       sp26-g-9.6.0.1(R).pck          /flash/sp26-g-9.6.0.1(R).pck
```

Step 4: Connect the extended cards Device3, Device4, and Device5 to the MVST domain, and detect that the version of Device3 is not consistent with the upgrade version, so upgrade automatically. If detecting that the versions of Device4 and Device5 are consistent, do not upgrade automatically.

#Connect Device3, Device4, and Device5 to the MVST domain, and then, check the MVST result on Device1.

#Check the MVST results on Device1. You can see that Device3, Device4, and Device5 join the MVST domain in the form of an extended card. The slots are Slave-slot0, Slave-slot1, and Save-slot2, and their host names change to switch-ss0, switch-ss1, and switch-ss2.

```
Device1#show mvst topo information
-------------------------------------------------------------------------------
-----------------------------------------
role     domain-name   interface       mac         device-type       host-name
-------------------------------------------------------------------------------
-----------------------------------------
Slave-slot  test       link-aggregation 1  0101.7a63.bd76   SFN3300-48Y8C    switch-ss0
Slave-slot  test       link-aggregation 2  0101.7a64.72aa   SFN3300-48Y8C    switch-ss1
Slave-slot  test       link-aggregation 3  0101.7a63.bd43   SFN3300-48Y8C    switch-ss2
Master    test              0101.7a6a.0258    SFN3300-48Y8C     Device1
```

#The upgrade status of the extended card can be checked in real time on Device1. Device3 is in the upgrade state. After the upgrade of Device3 is successful, the system restarts, but Device4 and Device5 are not upgraded.

```
Device1#show mvst upgrade-information slave-slot all
Slave slot upgrade information:
-------------------------------------------------------------------------------
-----------------------------------------
ss-id  upgrade-type  upgrade-status    start-time       over-time    hostname
-------------------------------------------------------------------------------
-----------------------------------------
0    image      downloading     JAN/27/2015 14:58:24          switch-ss0
```

```
1    none       none                    switch-ss1
2    none       none                    switch-ss2
```

#Device is upgrade successfully. Save the configuration and restart.

```
Device1#
%MVST-UPDATE_NOTIFY-5: Update slave slot 0 image successfully.
%MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
%MVST-NOTIFY_RELOAD-3: Slave slot 0 mpu is going to reload.
```

12.3.3.2 Configure Auto Delivering of Public Template

Network Requirements

- Device1 and Device2 form the stacking system and serve as MVST management device, and Device 3, Device 4 and Device 5 are used as extended cards, and the last two ports of the extended card are connected to the MVST management device;
- Configure Device3 as a template switch and its configuration serves as a public template configuration. When Device4 and Device5 are connected to the MVST domain, automatically deliver the configuration template;
- Change the configuration of Devce3, collect it as the public configuration template, and force it to be distributed to Device4 and Device5.

Network Topology

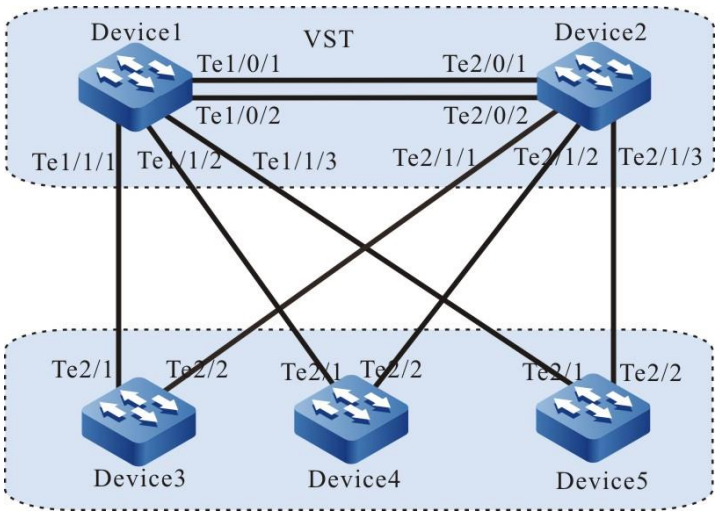


Figure 361 Configure the auto delivering of the public template

Configuration Steps

Step 1: Configure the VST system.

#On Device1, configure the No. of the virtual switch member device as 1, and the domain No. as 10, and the priority as 255.

```
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 255
Device1(config-vst-member-1)#exit
```

#On Device1, create virtual switch link interface 1, and add ports tentengigabitethernet0/1 and tentengigabitethernet0/2 to virtual switch link interface 1.

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tentengigabitethernet 0/1
Device1(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/1)#exit
Device1(config)#interface tentengigabitethernet 0/2
Device1(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/2)#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
```

#On Device2, configure the No. of the virtual switch member device as 2, the domain No. as 10, and the priority as 200.

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
```

```
Device2(config-vst-member-2)#exit
```

#On Device2, create virtual switch link interface 1, and add port tentengigabitethernet1/1 to virtual switch link interface 1.

```
Device2(config)#vsl-channel 1
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tentengigabitethernet 0/1
Device2(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/1)#exit
Device2(config)#interface tentengigabitethernet 0/2
Device2(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/2)#exit
```

#On Device2, save the configuration.

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

#Configure the running mode of Device1 as the 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!
%SYS-5-RELOAD: Reload requested
```

#Configure the running mode of Device2 as the stacking mode.

```
Device2#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!
%SYS-5-RELOAD: Reload requested
```

#View on Device1, the stacking system is formed, and Device1 is the master

device of the stacking system.

```
Device1#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode       : VIRTUAL
Virtual Switch DomainId    : 10
Virtual Switch mac-address : 0101.7a6a.0255

--------------- VST MEMBER INFORMATION -----------------
CODE MemberID Role   Pri    LocalVsl     RemoteVsl
-------------------------------------------------------------------------
L   1      Master   255  vsl-channel 1/1  vsl-channel 2/1
    2      Member  200  vsl-channel 2/1  vsl-channel 1/1
```

Step 2: Configure the MVST basic functions.

#Configure the stacking system as the MVST management device.

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

#Configure the link aggregation of the stacking system, and enable the MVST detection.

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

#On Device3, enable the MVST function.

```
Device3#configure terminal
Device3#configure terminal
Device3(config)#mvst enable
```

```
%MVST-NOTIFY-5: MVST is enabled !
Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.
```

#On Device4, enable the MVST function.

```
Device4#configure terminal
Device4(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device4(config)#mvst link-aggregation 2 mode lacp
Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active
Device4(config)#interface link-aggregation 2
Device4(config-link-aggregation2)#mvst inspection
Device4(config-link-aggregation2)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.
```

#On device5, enable the MVST function.

```
Device5#configure terminal
Device5(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device5(config)#mvst link-aggregation 3 mode lacp
Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active
Device5(config)#interface link-aggregation 3
Device5(config-link-aggregation3)#mvst inspection
Device5(config-link-aggregation3)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.
```

#Add Device3 to MVST domain as an extended card. Check the MVST results on Device1 after the device is added.

#Check the MVST results on Device1. You can see that Device3 joins the MVST domain in the form of an extended card. Its slot is Slave-slot0, and its host name changes to switch-ss0.

```
Device1#show mvst topo information
--------------------------------------------------------------------------------
```

```
-----------------------------------------
role     domain-name  interface        mac        device-type      host-name
-----------------------------------------------------------------------------------------
-----------------------------------------
Slave-slot  test        link-aggregation 1   0101.7a63.bd76  SFN3300-48Y8C   switch-ss0
Master    test                    0101.7a6a.0258   SFN3300-48Y8C    Device1
```

Step 3: Take Device3 as the template switch, and collect the public configuration template.

#Configure Device3.

```
Device1(config)#configure slave-slot 0
switch-ss0(config)#snmp-server host 1.1.1.1
switch-ss0(config)#snmp-server start
%SNMP-WARMSTART-5 SNMP agent on host switch-ss0 is undergoing a warm start
switch-ss0(config)#snmp-server enable traps vlan
switch-ss0(config)#link-aggregation 1
switch-ss0(config-link-aggregation1)#description management link
switch-ss0(config-link-aggregation1)#exit
switch-ss0(config)#vlan 100,200,300
```

#On Device1, check the configuration of the extended card Device3.

```
Device1#show running-config slave-slot 0
hostname switch-ss0

vlan 100,200,300
link-aggregation 1
 description management link
 no spanning-tree enable
 mvst inspection
 exit

snmp-server start
snmp-server view default 1.2 include
snmp-server view default 1.0.8802 include
snmp-server view default 1.1.2 include
snmp-server view default 1.3.111 include
snmp-server view default 1.3.6.1 include
snmp-server community public view default ro
snmp-server enable traps vlan
snmp-server host 1.1.1.1 traps community public version 2
```

#On Device1, save the configuration of Device3.

```
Device1#write slave-slot 0
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
```

```
Device1#
Jan  9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
```

Step 4: Take the configuration of Device3 as the public configuration template to deliver automatically.

#On Device1, configure the public configuration to deliver automatically.

```
Device1(config)#mvst configure template slave-slot 0
Are you sure to overwrite configure template /flash/mvst-template (Yes|No)?y
Get the slave slot 0 startup-config...OK
Write to /flash/mvst-template ....OK.
Device1(config)#
```

Step 5: Add the extended card to the MVST domain to load the configuration template automatically.

#Connect the extended card Device4 and Device5 to the MVST domain, and you can see the print information of automatically delivering the configuration template on Device1.

```
Device1#
%MVST-Slave_slot_add-5:Slave slot 1 add to the MVST
%MVST-Slave_slot_add-5:Slave slot 2 add to the MVST.
%MVST-EXECUTE_COFNIG-5:Slave slot 1 is going to execute configure template /flash/mvst-template.
%MVST-EXECUTE_COFNIG-5:Slave slot 1 execute configure file successfully!
%MVST-EXECUTE_COFNIG-5:Slave slot 2 is going to execute configure template /flash/mvst-template.
%MVST-EXECUTE_COFNIG-5:Slave slot 2 execute configure file successfully!
```

#On Device1, check the MVST result, and the host names of Device4 and Device5 are added with the suffix ss1 and ss2, that is, switch-ss1 and switch-ss2.

```
Device1#show mvst topo information
-------------------------------------------------------------------------------------------------------------
role      domain-name   interface        mac        device-type        host-name
-------------------------------------------------------------------------------------------------------------
Slave-slot  test        link-aggregation 1  0101.7a63.bd76  SFN3300-48Y8C    switch-ss0
Slave-slot  test        link-aggregation 2  0101.7a64.72aa  SFN3300-48Y8C    switch-ss1
Slave-slot  test        link-aggregation 3  0101.7a63.bd43  SFN3300-48Y8C    switch-ss2
Master    test                  0101.7a6a.0258   SFN3300-48Y8C     Device1
```

#On Device1, check the configuration of Device4, and the configuration is delivered successfully.

```
Device1#show running-config slave-slot 1
hostname switch-ss1

vlan 100,200,300

link-aggregation 1
 description management link
 no spanning-tree enable
 mvst inspection
 exit

snmp-server start
snmp-server view default 1.2 include
snmp-server view default 1.0.8802 include
snmp-server view default 1.1.2 include
snmp-server view default 1.3.111 include
snmp-server view default 1.3.6.1 include
snmp-server community public view default ro
snmp-server enable traps vlan
snmp-server host 1.1.1.1 traps community public version 2
```

#On Device1, check the configuration of Device5, and the configuration is delivered successfully.

```
Device1#show running-config slave-slot 2
hostname switch-ss2

vlan 100,200,300

link-aggregation 1
 description management link
 no spanning-tree enable
 mvst inspection
 exit

snmp-server start
snmp-server view default 1.2 include
snmp-server view default 1.0.8802 include
snmp-server view default 1.1.2 include
snmp-server view default 1.3.111 include
snmp-server view default 1.3.6.1 include
snmp-server community public view default ro
snmp-server enable traps vlan
snmp-server host 1.1.1.1 traps community public version 2
```

Step 6: Force the public configuration template to be delivered.

#Modify the configuration of Device3, and add the ACL configuration.

```
Device1(config)#configure slave-slot 0
switch-ss0(config)#ip access-list extended  test
switch-ss0(config-ext-nacl)#permit ip 192.168.0.1 0.0.0.255 any
switch-ss0(config-ext-nacl)#permit ip any any
switch-ss0(config-ext-nacl)#exit
switch-ss0(config)#end
switch-ss0#show access-list
ip access-list extended test
 10 permit ip 192.168.0.0 0.0.0.255 any
 20 permit ip any any
```

#On Device1, save the configuration of Device3.

```
Device1#write slave-slot 0
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
%MVST-WRITE_RESULT-5: The slave slot 0 write to startup file successfully.
%MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup begin.
%MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup OK.
```

#On Device1, re-collect the startup of Device3 as the new public configuration template.

```
Device1(config)#mvst configure template slave-slot 0
Are you sure to overwrite configure template /flash/mvst-template (Yes|No)?y
Get the slave slot 0 startup-config...OK
Write to /flash/mvst-template ....OK.
```

#On Device1, force the public configuration template to be distributed to Device4, and there is the printing information of successful distribution.

```
Device1(config)#mvst apply configure template slave-slot 1
%MVST-EXECUTE_COFNIG-5: Slave slot 1 is going to execute configure template /flash/ mvst-template
%MVST-EXECUTE_COFNIG-5: Slave slot 1 execute configure file successfully!
```

#Check if the configuration of Device4 contains the latest ACL configuration.

```
Device1(config)#configure slave-slot 1
switch-ss1#show access-list
ip access-list extended test
 10 permit ip 192.168.0.0 0.0.0.255 any
 20 permit ip any any
```

12.3.3.3 Configure Auto Delivering Bound Configuration

Network Requirements

- Device1 and Device2 form the stacking system and serve as MVST management device, and Device 3, Device 4, and Device 5 are used as extended cards, and the last two ports of the extended card are connected to the MVST management device;
- Perform the differentiated configuration for Device3, Device4 and Device5, and bind the configuration of the extended cards corresponding to link aggregation 1, link aggregation 2 and link convergence 3 to the MVST management device;
- After simulating the failure of Device3, replace a new device (Device6), and the MVST management device can automatically issue the previously collected Device3 configuration.
- It is simulated that when link aggregation 1 of MVST management device fails, link aggregation 4 needs to be created, and the configuration of Device3 bound to link aggregation group 1 is migrated to link aggregation 4.

Network Topology

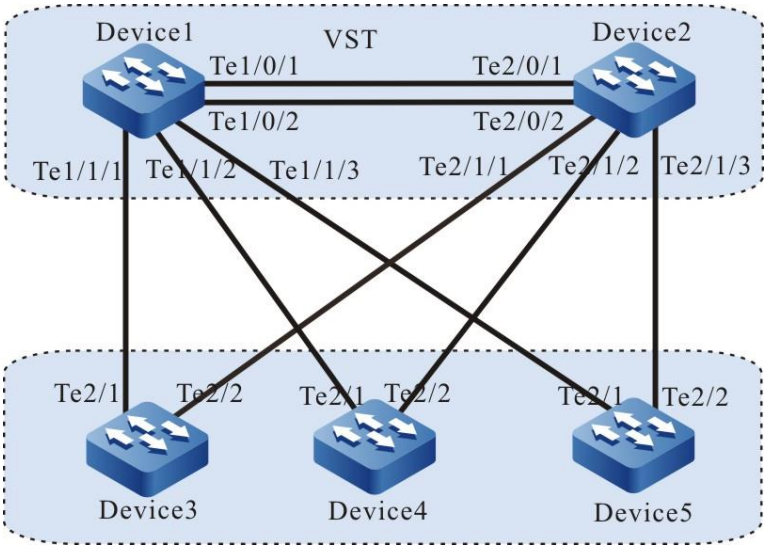


Figure 362 Configure auto delivering the bound configuration

Configuration Steps

Step 1: Configure the VST system.

#Configure virtual switch member device number as 1, domain number as 10 and priority as 255 on Device1.

```
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 255
Device1(config-vst-member-1)#exit
```

#On Device1, create virtual switch link interface 1, and add ports tentengigabitethernet0/1 and tentengigabitethernet0/2 to virtual switch link interface 1.

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tentengigabitethernet 0/1
Device1(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/1)#exit
Device1(config)#interface tentengigabitethernet 0/2
Device1(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device1(config-if-tentengigabitethernet0/2)#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
```

#Configure virtual switch member device number as 2, domain number as 10 and priority as 255 on Device2.

```
Device2#configure terminal
Device2(config)#switch virtual member 2
Do you want to modify member id(Yes|No)?y
% Member ID 2 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device2(config-vst-member-2)#priority 200
Device2(config-vst-member-2)#exit
```

#On Device2, create virtual switch link interface 1, and add ports

tentengigabitethernet1/1 to virtual switch link interface 1.

```
Device2(config)#vsl-channel 1
Device2(config-vsl-channel-1)#exit
Device2(config)#interface tentengigabitethernet 0/1
Device2(config-if-tentengigabitethernet0/1)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/1)#exit
Device2(config)#interface tentengigabitethernet 0/2
Device2(config-if-tentengigabitethernet0/2)#vsl-channel 1 mode on
Device2(config-if-tentengigabitethernet0/2)#exit
```

#On Device2, save the configuration.

```
Device2#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

#Configure the running mode of Device1 as the 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!
%SYS-5-RELOAD: Reload requested
```

#Configure the running mode of Device2 as the stacking mode.

```
Device2#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!
%SYS-5-RELOAD: Reload requested
```

#View on Device1, the stacking system is formed, and Device1 is the master device of the stacking system.

```
Device1#show switch virtual
```

```
Codes: L - local-device,I - isolate-device

Virtual Switch Mode       : VIRTUAL
Virtual Switch DomainId   : 10
Virtual Switch mac-address : 0101.7a6a.0255

--------------- VST MEMBER INFORMATION ---------------------
CODE MemberID Role    Pri  LocalVsl       RemoteVsl
------------------------------------------------------------------------------
L   1      Master   255  vsl-channel 1/1 vsl-channel 2/1
    2      Member   200  vsl-channel 2/1 vsl-channel 1/1
```

Step 2: Configure the MVST basic functions.

#Configure the stacking system as the MVST management device.

```
Device1(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device1(config)#mvst master
Device1(config)#mvst domain-name test
```

#Configure the link aggregation of the stacking system, and enable the MVST detection.

```
Device1(config)#mvst link-aggregation 1 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/1,2/1/1 join link-aggregation 1 active
Device1(config)#interface link-aggregation 1
Device1(config-link-aggregation1)#mvst inspection
Device1(config-link-aggregation1)#exit
Device1(config)#mvst link-aggregation 2 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/2,2/1/2 join link-aggregation 2 active
Device1(config)#interface link-aggregation 2
Device1(config-link-aggregation2)#mvst inspection
Device1(config-link-aggregation2)#exit
Device1(config)#mvst link-aggregation 3 mode lacp
Device1(config)# mvst interface tengigabitethernet 1/1/3,2/1/3 join link-aggregation 3 active
Device1(config)#interface link-aggregation 3
Device1(config-link-aggregation3)#mvst inspection
Device1(config-link-aggregation3)#exit
```

#On Device3, enable the MVST function.

```
Device3#configure terminal
Device3#configure terminal
Device3(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device3(config)#mvst link-aggregation 1 mode lacp
Device3(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 1 active
```

```
Device3(config)#interface link-aggregation 1
Device3(config-link-aggregation1)#mvst inspection
Device3(config-link-aggregation1)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 1 successfully.
```

#On Device4, enable the MVST function.

```
Device4#configure terminal
Device4(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device4(config)#mvst link-aggregation 2 mode lacp
Device4(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 2 active
Device4(config)#interface link-aggregation 2
Device4(config-link-aggregation2)#mvst inspection
Device4(config-link-aggregation2)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 2 successfully.
```

#On Device5, enable the MVST function.

```
Device5#configure terminal
Device5(config)#mvst enable
%MVST-NOTIFY-5: MVST is enabled !
Device5(config)#mvst link-aggregation 3 mode lacp
Device5(config)# mvst interface tengigabitethernet 2/1,2/2 join link-aggregation 3 active
Device5(config)#interface link-aggregation 3
Device5(config-link-aggregation3)#mvst inspection
Device5(config-link-aggregation3)#exit

%MVST-NOTIFY-5: interface tengigabitethernet2/1 and interface tengigabitethernet2/2 join link-aggregation 3 successfully.
```

#Connect Device3, Device4, and Device5 to the MVST domain, and then, check the MVST result after the devices are connected.

#Check the MVST results on Device1. You can see that Device3, Device4, and Device5 join the MVST domain in the form of an extended card. The slots are Slave-slot0, Slave-slot1, and Save-slot2, and their host names change to switch-ss0, switch-ss1, and switch-ss2.

```
Device1#show mvst topo information
-------------------------------------------------------------------------------------------------------
role    domain-name    interface        mac        device-type        host-name
```

```
-------------------------------------------------------------------------------
-----------------------------------------
Slave-slot  test        link-aggregation 1  0101.7a63.bd76  SFN3300-48Y8C   switch-ss0
Slave-slot  test        link-aggregation 2  0101.7a64.72aa  SFN3300-48Y8C   switch-ss1
Slave-slot  test        link-aggregation 3  0101.7a63.bd43  SFN3300-48Y8C   switch-ss2
Master    test                    0101.7a6a.0258  SFN3300-48Y8C    Device1
```

Step 3: Configure the function of auto delivering the bound configuration.

#Perform the differentiated configuration for Device3, Device4, and Device5.

```
Device1(config)#configure slave-slot 0
switch-ss0(config)#vlan 100
switch-ss0(config)#exit
switch-ss0#exit
switch-ss0>exit
Device1(config)#configure slave-slot 1
switch-ss1(config)#vlan 200
switch-ss1(config)#exit
switch-ss1#exit
switch-ss1>exit
Device1(config)#configure slave-slot 2
switch-ss2(config)#vlan 300
switch-ss2(config)#exit
switch-ss2#exit
switch-ss2>exit
```

#On Device1, save the configurations of Device3, Device4, and Device5.

```
Device1#write slave-slot 0
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan   9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 0 write to startup file
successfully.
Device1#write slave-slot 1
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan   9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 1 write to startup file
successfully.
Device1#write slave-slot 2
Are you sure to overwrite slave slot 0 /flash/startup (Yes|No)?y
Device1#
Jan   9 2015 16:32:34: %MVST-WRITE_RESULT-5: The slave slot 2 write to startup file
successfully.
```

#Configure the function of auto delivering the bound configuration on Device1. The startup of the extended cards corresponding to link aggregation group 1, link aggregation group 2 and link aggregation group 3 is collected to the MVST

management device.

```
Device1(config)#mvst bind startup link-aggregation 1
Device1(config)#
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup begin.
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 0 startup OK.
Device1(config)#mvst bind startup link-aggregation 2
Device1(config)#
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 1 startup begin.
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 1 startup OK.
Device1(config)#mvst bind startup link-aggregation 3
Device1(config)#
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 2 startup begin.
Jan  9 2015 15:25:16: %MVST-COLLECT_STARTUP-5: Collect slave slot 2 startup OK.
```

#View the results of auto delivering the bound configuration on Device1. The startup of extended cards 0, 1 and 2 are collected into the startup-lag1, startup-lag2, and startup-lag3 files in USB.

```
Device1#show mvst startup bind info
-------------------------------------------------
Interface            Bind-file-name
-------------------------------------------------
link-aggregation 1     /usb/startup-lag1
link-aggregation 2     /usb/startup-lag2
link-aggregation 3     /usb/startup-lag3
```

#After enabling the MVST function on a new device (Device6), the link aggregation group 1 of the MVST management device is added to the MVST domain to replace Device3. Device6 is added to the MVST domain in the form of an extended card. The slot is Slave-slot3, and there is the print information of auto delivering startup-lag1 configuration.

```
Device1#
Jan  9 2015 16:54:46: %MVST-Slave_slot_add-5:Slave slot 3 add to the MVST.
Jan  9 2015 16:54:47: %MVST-EXECUTE_COFNIG-5: Slave slot 3 is going to execute configure file /usb/ startup-lag1.
Jan  9 2015 16:54:48: %MVST-EXECUTE_COFNIG-5: Slave slot 3 execute configure file successfully!
```

#Check the MVST results on Device1. Device6 joins the MVST domain in the form of an extended card. Its slot is Slave-slot3, and its host name is switch-ss3.

```
Device1#show mvst topo information
-------------------------------------------------------------------------------------
---------------------------------------
```

```
role    domain-name    interface       mac        device-type      host-name
-------------------------------------------------------------------------------
-------------------------------------
Slave-slot  test        link-aggregation 4  0101.7a63.bd89  SFN3300-48Y8C   switch-ss3
Slave-slot  test        link-aggregation 2  0101.7a64.72aa  SFN3300-48Y8C   switch-ss1
Slave-slot  test        link-aggregation 3  0101.7a63.bd43  SFN3300-48Y8C   switch-ss2
Master    test                  0101.7a6a.0258  SFN3300-48Y8C   Device1
```

#Check the configuration of Device6, Device6 loads the configuration of Device3, and VLAN100 is created.

```
Device1#show run slave-slot 3
vlan 100
```

Step 4: Configure the function of migrating auto delivered bound configuration.

#On Device1, configure link aggregation 4.

```
Device1(config)#interface tengigabitethernet 1/1/1,2/1/1
Device1(config-if-range)#link-aggregation 4 active
Device1(config-if-range)#exit
```

#Configure the migration of auto delivered bound configuration on Device1, migrating the configuration collected by link aggregation 1 to link aggregation 4.

```
Device1(config)#mvst bind startup link-aggregation 4
Device1(config)#mvst relocate configure interface link-aggregation 1 interface link-
aggregation 4
interface link-aggregation1 file will cover interface link-aggregation4 file, are you sure to do
it(Yes|No)?y
```

#On Device1, check if the result configuration is migrated successfully, and there is the configuration file named startup-lag4 in USB.

```
Device1(config-fs)#cd /usb
Device1(config-fs)#dir
7256          JAN-09-2015  17:58:16   startup-lag4
```

#Delete the startup of Device6, restart Device6 without saving the configuration. After the device is started, you can see that the configuration of startup-lag4 is loaded on Device6, which is consistent with the configuration of startup-lag1 before migration.

```
Device1#show run slave-slot 3
vlan 100
```

13 Data Center Feature

13.1VXLAN

13.1.1 Overview

13.1.1.1 Background

In order to achieve high reliability and redundant deployment, most enterprise networks and their data centers cross multiple physical sites in different physical locations, and deploy similar services at these sites. In order to integrate the data center resources and reduce the management cost, the data center resources are usually virtualized. The virtualization technology of data center mainly includes network virtualization, storage virtualization and server virtualization. Among them, server virtualization is to use special virtualization software to virtualize multiple virtual machines on a physical server. Each virtual machine runs independently and has its own operating system, application program and virtual hardware environment. In order to realize the dynamic resource allocation and management between sites, virtual machines should be able to migrate freely between data centers. Because the migration process of virtual machines is transparent to users, IP address cannot be changed. Therefore, the networks before and after the migration of virtual machines is required to be in the same L2 network. Therefore, it is necessary to realize the interconnection of L2 networks among sites distributed in different places.

VXLAN is a kind of "MAC in IP" technology, which is used to realize the big L2 interconnection based on IP core network. VXLAN only maintains MAC address and forwarding information on the edge devices of the site, without changing the internal network and core network structure of the site.

Using VXLAN as the big L2 network interconnection technology has the following advantages:

- The VXLAN encapsulates the packets sent by the virtual machine in UDP, and uses the IP/MAC address of the physical network as the outer header

to encapsulate, which only shows the encapsulated parameters. Therefore, the requirement of the big L2 network for the MAC address specification is greatly reduced. In addition to vxlan network edge devices, the other devices in the network do not need to identify the MAC address of the virtual machine, which reduces the pressure of MAC address learning and improves the performance of the device.

- The VXLAN introduces a user ID similar to VLAN ID, which is called VXLAN network identifier VNI. It is composed of 24 bits and supports up to 16777215 VXLAN segments, so as to meet a large number of user IDs.
- By using MAC in UDP encapsulation to extend the L2 network, the physical network and virtual network are decoupled. Tenants can plan their own virtual network without considering the limitations of physical network IP address and broadcast domain, which greatly reduces the difficulty of network management.

13.1.1.2 Basic Concepts

Network Virtual Edge Node

NVE (network virtualization edge) is a network entity that realizes the function of network virtualization. After the packet is encapsulated and transformed by the NVE network entity, the virtual VXLAN network can be established between the NVE based on the three-layer basic network.

VXLAN Tunnel End Point

VTEP (VXLAN Tunnel End Point) is a switching device located at the edge of the site. It operates as a layer-2 device in the site network and a L3 device in the core network. It mainly provides two-layer interconnection between site networks. It completes the packet encapsulation from the site network to the core network, and the packet de-encapsulation from the core network to the site network.

Core network interface: The L3 interface on the edge device connected to the core

network, namely Network Port.

Site internal interface: The L2 interface on the edge device connected to the internal device of the site, namely Internal Port.

VXLAN Session

VXLAN session is to establish the VXLAN tunnel through manual configuration or protocol negotiation, and associate VXLAN instance to form an effective forwarding instance between VTEPs. This instance is called VXLAN session. Data can only be forwarded if the vxlan session is valid.

EVPN

EVPN (Ethernet Virtual Private Network) is a L2 VPN technology. The EVPN technology uses the extended MP-BGP to spread the host information in the user network among different sites, and uses the control plane to replace the data plane to complete the cross-site MAC address learning in the user network.

VXLAN is just a data encapsulation protocol. It does not define control plane. MAC address learning between sites is completed by the traffic flooding of the traditional data plane. The biggest drawback of this method is that there is a lot of flooding traffic in the data center bearing network. In order to solve this problem, VXLAN introduces EVPN as the control plane. By exchanging BGP EVPN routes between VTEPs, it realizes the auto discovery of VTEP and the mutual notification of host information, so as to avoid unnecessary data flooding.

13.1.1.3 Protocol Specifications

- RFC7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks.
- RFC 7432: BGP MPLS-Based Ethernet VPN
- RFC 8365--A Network Virtualization Overlay Solution Using Ethernet

VPN (EVPN)

- draft-ietf-bess-evpn-inter-subnet-forwarding-05
- draft-ietf-bess-evpn-prefix-advertisement-11
- draft-malhotra-bess-evpn-irb-extended-mobility-03

13.1.2 VXLAN Function Configuration

Table 1586 VXLAN function configuration list

Configuration Tasks	
Configure VXLAN basic functions	Configure VXLAN instance
	Configure VXLAN instance description information
	Configure the BUM packet speed limit function of the VXLAN instance
	Configure the function of de-encapsulating the VXLAN tunnel on the port/interface
	Configure VXLAN L3 interface
	Configure NVE
	Enable the ARP host advertising
	Enable ARP broadcast suppression
	Enable IPv6 host advertising
	Enable IPv6 multicast suppression
Configure the static VXLAN	Configure the copy list of the VXLAN static header
Configure EVPN VXLAN	Configure NVE to enable EVPN
	Configure the EVPN attributes of the VXLAN instance
	Configure the EVPN attributes of the VRF instance (optional)
	Configure BGP to enable EVPN
	Configure the BGP neighbor policy (optional)
	Configure VXLAN route map (optional)

13.1.2.1 Configure VXLAN Instance

Configuration Condition

None

Configure VXLAN Instance

Each VXLAN instance is an independent working area. Through VNID isolation, different VXLAN instances cannot communicate with each other. The same VXLAN instance can communicate with each other. The device supports configuration of up to 4096 VXLAN instances.

Table 1587 Configure the VXLAN instance

Step	Command	Description
Global configuration mode	configure terminal	-
VXLAN configuration mode	vxlan *vxlan-id*	Mandatory By default, do not create any VXLAN.
Configure VXLAN VNID	vxlan vnid *vnid*	By default, it is not configured.

Note

- The VNID of VXLAN instance must be configured in priority. Otherwise, other service configurations will not take effect.

Configure VXLAN Instance Description Information

To be convenient for memory and management, the description information of VXLAN can be configured according to the service type, function and connection of VXLAN.

Table 1588 Configure the VXLAN description information

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	Mandatory After entering the VXLAN configuration mode, the VXLAN description

Step	Command	Description
		information can be configure.
Configure VXLAN description information	description *description-name*	Optional By default, VXLAN does not have the description information.

VXLAN Instance Service Access

VXLAN does not contain any service access points when it is initially created. Virtual machines are connected to the VXLAN network by using different access modes, so as to realize VXLAN network forwarding for virtual machine services. The access mode is as follows:

Table 1589 Configure the service point mode

Mode	Description
default	Permit the interface to receive all packets, regardless of whether there is VLAN tag in the packet. Whether VXLAN encapsulating or de-encapsulating the original packet, this type of interface will not perform any VLAN tag processing on the original packet, including adding, replacing or stripping. This mode only supports L2 Forwarding and does not support cross-VXLAN forwarding
untag	This type of interface only receives the packets without VLAN tag This mode supports both L2 Forwarding and L3 forwarding
dot1q	This type of interface only receives the packets with VLAN tag and the outer VLAN tag matching the specified VLAN tag; When vxlan encapsulates the original packet, this type of interface will peel off the outermost VLAN tag; When unpacking vxlan packets, the specified VLAN tag will be added before forwarding. In this mode, it is necessary to add the physical port to the corresponding VLAN, and create the global VLAN. This mode supports both L2 Forwarding and L3 forwarding.
qinq	This type of interface only receives the packets with specified two layers of VLAN tags; When vxlan encapsulates the original packet, this type of interface will peel off the two outermost VLAN tags;

Mode	Description
	When de-encapsulating vxlan packets, add the specified two layers of VLAN tags before forwarding. In this mode, it is necessary to add the physical port to the corresponding outer VLAN, and create the global VLAN. This mode supports both L2 forwarding and L3 forwarding.

The VXLAN instance does not contain any service access points when it is initially created. You need to manually configure it as follows.

Table 1590 Configure the service point

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the port mode	interface tengigabitethernet 0/1	Mandatory After entering the port mode, you can configure the port to be added to the VXLAN instance, supporting the aggregation port.
Configure the VXLAN instance access mode	vxlan *vxlan-id* encapsulation { vlan *vlan-id* | qinq svlan *svlan-id* cvlan *cvlan-id* | untag | default }	Mandatory By default, no port is added to VXLAN. After the port is added to the VLAN, VXLAN function can take effect on the port.

Note

- When the access mode is untag and defaul, multiple vxlan instances cannot be added to the same port at the same time.
- When the access mode is VLAN mode, the vxlan access port needs to be configured as tag access

Configure BUM Packet Speed Limit Function of VXLAN Instance

VXLAN does not contain any BUM (unknown unicast, multicast, broadcast) packet suppression function when it is initially created. After this function is enabled, you can limit the speed of the BUM packets.

Table 1591 Configure the service point mode

Type	Description
broadcast-suppression	Limit the speed of the broadcast packets
multicast-suppression	Limit the speed of the multicast packets
unicast-suppression	Limit the speed of the unknown unicast packets
all-flooding	Suppress the BUM packets

The VXLAN instance does not contain any BUM packet speed limit when it is initially created. You need to perform the following configuration manually.

Table 1592 Configure the service point

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure VXLAN instance mode	vxlan 100	Mandatory Enter the VXLAN instance mode, and then, you can configure the BUM packet speed limit.
Configure the BUM packet speed limit of the VXLAN instance	vxlan { broadcast-suppression | multicast-suppression | unicast-suppression}cir *cirvalue* cbs *cbsvalue*	Optional By default, do not limit the speed of any BUM packet.
Configure the BUM packet suppression function of the VXLAN instance	vxlan all-flooding	Optional By default, do not suppress any BUM packets.

Configure Port/L3 Ethernet Interface to De-encapsulate the VXLAN Tunnel

After any L2 Ethernet interface/L3 Ethernet interface/aggregation group/L3

aggregation interface enables the function, it can be used to de-encapsulate the VXLAN tunnel.

Table 1593 Configure the service point

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the port/interface mode	interface tengigabitethernet 0/1	Mandatory Enter the port/interface mode, and then you can configure the port VXLAN de-encapsulation function, supporting the aggregation port.
Configure the function of de-encapsulating the VXLAN tunnel	vxlan decapsulation	Optional By default, no port enables the function of de-encapsulating the VXLAN tunnel.

Configure VXLAN L3 Interface

When enabling the L3 VXLAN function, you should configure the VXLAN L3 interface and specify IP.

Table 1594 Configure the VXLAN interface

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure VXLAN interface	interface vxlan *vxlan-id*	Mandatory By default, do not configure the VXLAN interface. When the L3 VXLAN function is enabled, it must be configured.
Configure the VXLAN interface to associate with VRF	ip vrf forwarding *vrf-name*	Optional By default, the VXLAN interface is not associated with vrf.
Configure the IP address of the	ip address *X.X.X.X*	Mandatory

Step	Command	Description
VXLAN interface		By default, the VXLAN interface is not configured with IP address. When the L3 VXLAN function is enabled, it must be configured.

Configure NVE

NVE (network virtualization edge) is a network entity that realizes the function of network virtualization. After the packet is encapsulated and transformed by the NVE network entity, the virtual VXLAN network can be established between the NVEs based on the L3 basic network.

Table 1595 Configure nve

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create one nve interface	interface nve *nve-number*	Mandatory By default, do not create the NVE interface on the device.
Configure the source IP address	source *ip-address*	Mandatory By default, the VTEP IP address is not configured on the NVE interface.
Configure source IPv6 address	source *ipv6-address*	It is mandatory when the IPv6 tunnel is enabled. By default, VTEP IPv6 address is not configured on NVE interface.

Enable ARP Host Advertising

After enabling the ARP host advertising function in VXLAN instance, the ARP request packet, ARP response packet and free ARP packet received on the user port will generate a local ARP host table and advertise it to EVPN routing, and then advertise it to neighbors through BGP EVPN protocol to realize route learning between VTEPs and install ARP broadcast suppression table.

Table 1596 Enable ARP host advertising

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	Mandatory
Enable ARP host advertising	arp host advertise	Mandatory By default, do not enable ARP host advertising.

Enable ARP Broadcast Suppression

After VXLAN enables the ARP broadcast suppression function, after receiving the ARP broadcast request packet on the user side port, use the request destination IP to query the ARP broadcast suppression table. The ARP broadcast request packet that hits the suppression table can be answered on behalf or transferred to unicast; The ARP broadcast request packet that does not hit the suppression table can be broadcasted or discarded.

After the ARP broadcast suppression function is enabled, the broadcast packet in VXLAN domain can be reduced.

Table 1597 Enable the ARP broadcast suppression

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	Mandatory
Enable the ARP broadcast suppression function	arp suppression	Mandatory By default, the broadcast suppression function is disabled.
Configure transferring to unicast after hitting the suppression table,.	arp suppression unicast forward	Optional By default, the ARP request packet that hits the suppression table is answered on behalf.

Step	Command	Description
Configure discarding after not hitting the suppression table.	arp suppression mismatch discard	Optional By default, the ARP request packet that does not hit the suppression table is broadcasted.

Enable IPv6 Host Advertising

After enabling the IPv6 host advertising function in VXLAN instance, the NS and NA packets of IPv6 received on the user port will generate a local IPv6 host table and advertise it to EVPN routing, and then advertise it to neighbors through BGP EVPN protocol to realize route learning between VTEPs and install IPv6 multicast suppression table.

Table 1598 Enable IPv6 host advertising

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	Mandatory
Enable IPv6 host advertising	nd host advertise	Mandatory By default, do not enable IPv6 host advertising.

Enable IPv6 Multicast Suppression

After vxlan enables the IPv6 Multicast suppression function, after receiving the NS multicast request packet on the user side port, use the request destination IPv6 address to query the multicast suppression table. The NS multicast request packet that hits the suppression table can be answered on behalf or transferred to unicast; The NS multicast request packet that does not hit the suppression table can be multicasted or discarded.

After enabling IPv6 multicast suppression function, multicast packets in vxlan domain can be reduced.

Table 1599 Enable IPv6 multicast suppression

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the VXLAN configuration mode	vxlan *vxlan-id*	Mandatory
Enable IPv6 multicast suppression function	nd suppression	Mandatory By default, the broadcast suppression function is disabled.
Configure transferring to unicast after hitting the suppression table,.	nd suppression unicast forward	Optional By default, the NS request packet that hits the suppression table is answered on behalf.
Configure discarding after not hitting the suppression table.	nd suppression mismatch discard	Optional By default, the NS request packet that does not hit the suppression table is broadcasted.

13.1.2.2 Configure Static VXLAN Tunnel

Configuration Condition

None

Configure Static Header Copy List of VXLAN Instance

The header refers to the ingress node of the VXLAN tunnel, and the copy list refers to that when the incoming node of the VXLAN tunnel receives the BUM (Broadcast&Unknown-unicast&Multicast) packet, it will copy the packet and send it to all VTEPs in the list. The header copy list is the IP address list of the remote VTEP used to guide the ingress node of VXLAN tunnel to copy and send the BUM packet.

The header copy list, also known as the BUM VXLAN tunnel, copies the received

BUM packet according to the VTEP list and sends it to all VTEPs belonging to the same VNI through the header copy list source NVE interface.

Table 1600 Configure the copy list of the VXLAN static header

Step	Command	Description
Global configuration mode	configure terminal	-
NVE interface configuration mode	interface nve *nve-number*	Mandatory
Configure the copy list of the specified VXLAN static header	vxlan *vxlan-id* ingress-replication peer {*ip-address* | *ipv6-address* }	Mandatory By default, do not configure the copy list of the static header.

Note

- Even if the source VTEP only corresponds to one remote VTEP, it is necessary to execute the command to specify the corresponding VTEP address and configure the header copy list.

13.1.2.3 Configure EVPN VXLAN Tunnel

Configuration Condition

Before configuring the BGP EVPN mode to deploy the VXLAN service, first complete the following tasks:

- Configure the link-layer protocol, ensuring the normal communication of the link layer
- Configure the network-layer address of the interface, making the neighboring network node reachable at the network layer

Configure NVE to Enable the EVPN Protocol

After NVE activates EVPN, automatically negotiate and set up the VXLAN

tunnel automatically between VTEPs via the BGP EVPN protocol.

Table 1601 Configure the dynamic VXLAN tunnel

Step	Command	Description
Global configuration mode	configure terminal	-
NVE interface configuration mode	interface nve *nve-number*	Mandatory
Configure the specified VXLAN instance to associate NVE	vxlan *vxlan-id*	Mandatory By default, do not associate.
Specify the VXLAN instance to use EVPN to set up the header copy list	vxlan *vxlan-id* ingress-replication protocol bgp	Optional By default, do not specify.

Configure the EVPN Attributes of the VXLAN Instance

RD is used to identify EVPN routes generated by different VXLANs, so as to achieve isolation between different VXLANs; route-target is used to control the import and export of EVPN routes. When VTEP initiates EVPN routes, it carries the Export RT attribute. When VTEP decides to which VXLAN the EVPN route is imported, the Export RT attribute carried by the route is used to match the Import RT of the local VXLAN.

Table 1602 Configure the VXLAN EVPN attributes

Step	Command	Description
Global configuration mode	configure terminal	-
VXLAN instance configuration mode	vxlan *vxlan-id*	Mandatory In the VXLAN configuration mode, you can enter the EVPN configuration mode.
VXLAN EVPN configuration mode	address-family evpn	Mandatory After entering the VXLAN EVPN mode, you can configure the VXLAN EVPN attributes.
Configure VXLAN rd	rd *route-distinguisher*	Mandatory

Step	Command	Description
		By default, do not configure VXLAN RD.
Configure VXLAN route-target	route-target [both|export|import] { *ASN:nn|IP-address:nn*}	Mandatory By default, do not configure the Export, Import RT attributes of VXLAN.

Configure the EVPN Attributes of the VRF Instance (Optional)

Only when the distributed gateway is deployed, the EVPN attribute of VRF instance needs to be configured. This configuration is ignored in centralized gateway deployment.

Table 1603 Configure the EVPN attributes of the VRF instance

Step	Command	Description
Global configuration mode	configure terminal	-
Enter the VRF configuration mode	ip vrf *vrf-name*	Mandatory
Configure rd	rd *route-distinguisher*	Mandatory By default, do not configure rd.
Configure L3VNID	l3vnid *vnid-number*	Mandatory By default, it is not configured.L3VNID.
Enter the VRF EVPN address family configuration mode	address-family evpn	Mandatory
Configure the route-target of VRF EVPN	route-target [both | export | import] { *ASN:nn|IP-address:nn*}[ipv4 | ipv6]	Mandatory By default, do not configure the Import and Export attribute.
Associate VRF EVPN with the egress route policy.	export map *route-map-name* [ipv4 | ipv6]	Optional By default, VRF EVPN is not associated with the egress route policy.
Associate VRF EVPN with	import map *route-map-name*	Optional

Step	Command	Description
the ingress route policy.	[ipv4 | ipv6]	By default, VRF EVPN is not associated with the ingress route policy.

Configure BGP to Enable EVPN

BGP enables the EVPN capability, making BGP learn the EVPN route, create dynamic VXLAN tunnel, form the VXLAN session and add to the forwarding table, and guide the VXLAN packet forwarding.

Table 1604 Configure BGP EVPN to enable EVPN

Step	Command	Description
Global configuration mode	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode	router bgp *autonomous-system*	Mandatory By default, it is not enabled.
Configure the BGP neighbor	neighbor { *neighbor-address* | *peer-group-name* } remote-as *as-number*	Mandatory By default, do not create any BGP neighbor.
Configure the source address of the TCP session of the BGP neighbor	neighbor { *neighbor-address* | *peer-group-name* } update-source { *interface-name* | *ip-address*|*ipv6-address* }	Optional By default, TCP sessions automatically select the address of the route egress interface as the source address.
Enter the BGP EVPN configuration mode	address-family l2vpn evpn	Mandatory
Activate the EVPN capability	neighbor { *neighbor-address* | *peer-group-name* } activate	Mandatory By default, it is not activated.
Configure the EVPN reflector	neighbor { *neighbor-address* | *peer-group-name* } route-reflector-client	Optional By default, do not enable the reflector.
Enter the BGP IPV4 VRF configuration mode	address-family {ipv4|ipv6} vrf *vrf-name*	Optional

Step	Command	Description
Configure VRF unicast route to be re-distributed to EVPN and form five types of routes	advertise-l2vpn-evpn	Optional This configuration is required for the deployment of the distributed gateway.
Enter the BGP EVPN configuration mode	address-family l2vpn evpn	Mandatory
When BGP is configured to announce routes to neighbors or peer groups, do not change the as path, Med, and next hop attribute values of the route.	neighbor attribute-unchanged[as-path | med | next-hop]	Optional This configuration is only required when deploying an end-to-end cross-data center VXLAN network.

Configure BGP Neighbor Policy (Optional)

By binding the route map on the BGP EVPN neighbors, you can filter the routes with the specified VNI received in the ingress direction effectively, or prevent advertising some routes with the specified VNI to the neighbors in the egress direction.

Table 1605 Configure the EVPN policy of the BGP neighbor

Step	Command	Description
Global configuration mode	configure terminal	-
Enable the BGP protocol and enter the BGP configuration mode	router bgp *autonomous-system*	Mandatory By default, do not enable BGP.
Enter the BGP EVPN configuration mode	address-family l2vpn evpn	Mandatory
Configure the neighbor to apply the route map in the ingress direction	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* in	Mandatory By default, do not apply the route map in the ingress direction.
Configure the neighbor to apply the route map in the egress direction	neighbor { *neighbor-address* | *peer-group-name* } route-map *rtmap-name* out	Mandatory By default, do not apply the route map in the egress

Step	Command	Description
		direction.

Configure VXLAN Route Map (Optional)

When configuring the neighbor VXLAN policy, it is necessary to bind the route map, and use the route map to match the local VXLAN number, route next hop and other matching items to control the ingress and egress routes.

Table 1606 Configure the VXLAN route map

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Create the route map	route-map *map-name* [{ permit | deny } [*seq-number*]]	Mandatory By default, do not create the route map.
Match vxlan-id	match vxlan *vxlan-id*	Optional By default, do not match the local VXLAN No.

13.1.2.4 VXLAN Monitoring and Maintaining

Table 1607 VXLAN monitoring and maintaining

Command	Description
clear arp host vxlan [all | *vxlan-id* [*ip-address*]]	Clear the local ARP host information in the VXLAN instance
clear nd host vxlan [all | *vxlan-id* [*ip-address*]]	Clear the local IPv6 host information in the VXLAN instance
show arp host vxlan [*vxlan-id*]	View the local ARP host information in the VXLAN instance
show arp suppression [vxlan *vxlan-id*]	View the ARP broadcast

	suppression table in the VXLAN instance
show bgp l2vpn evpn { all | rd *route-distinguisher* |*vxlan-id* } neighbors *neighbor-address* { advertised-routes | received-routes | routes} { all-type | type 2 | type 3| type 5 }	Display the route information of the specified neighbor under the BGP EVPN address cluster
show bgp l2vpn evpn *vxlan-id* statistics	Display the routing statistics of the specified VXLAN under the BGP EVPN address cluster
show bgp l2vpn evpn summary	Display neighbor summary information of BGP EVPN
show nd host vxlan	View the local IPv6 host information in the VXLAN instance
show nd suppression [vxlan *vxlan-id*]	View the IPv6 multicast suppression table in the VXLAN instance
show vxlan [*vxlan-id*] config	Display the configuration information for a specified VXLAN instance
show vxlan *vxlan-id* instance	Display the instance information of the specified VXLAN
show vxlan *vxlan-id* internal	Display the service access point of the specified VXLAN instance
show vxlan *vxlan-id* session	Displays all session information associated with the specified VXLAN instance
show vxlan config	Display the global information of VXLAN
show vxlan instance	Display the VXLAN instance information
show vxlan internal [interface *interface-num* | interface link-aggregation *link-aggregation-id*]	Display the VXLAN service success point
show vxlan tunnel	Display the VXLAN tunnel information

show vxlan session	Display the VXLAN session information

13.1.3 VXLAN Typical Configuration Example

13.1.3.1 Configure Static VXLAN to Realize L2 Intercommunication

Network Requirements

- Leaf1 and leaf2 serve as VTEP to create the VXLAN instance.
- Leaf1 and Leaf2 set up the static VXLAN tunnel through loopback interface.
- The VXLAN tunnel is established to realize the VM interworking between server 1 and server2 of the same network segment.

Network Topology

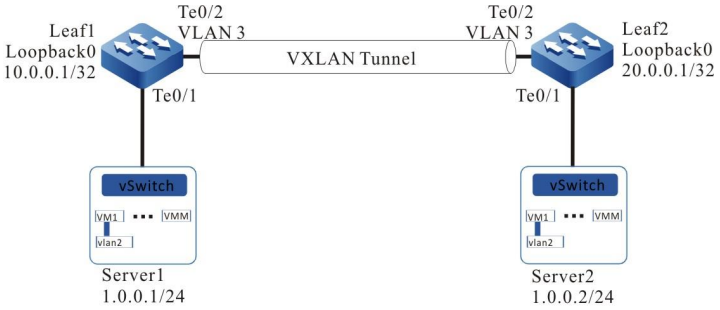


Figure 363 Networking of configuring the static VXLAN to realize the L2 intercommunication

Configuration Steps

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

Step 2: Configure the IP address of the interface.

#Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

#Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 3
Leaf2(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Leaf2(config-if-vlan3)#exit
```

Step 3: Configure OSPF, making the Loopback routes between the devices reachable.

#Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

#Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

#View the route table of Leaf1.

```
Leaf1#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, 00:05:40, vlan3
C   127.0.0.0/8 is directly connected, 1d:21:38:36, lo0
C   10.0.0.1/32 is directly connected, 00:06:34, loopback0
O   20.0.0.1/32 [110/2] via 2.0.0.2, 00:00:05, vlan3
```

#View the route table of Leaf2.

```
Leaf2#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, 00:06:43, vlan3
C   127.0.0.0/8 is directly connected, 1w3d:03:35:57, lo0
O   10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:36, vlan3
C   20.0.0.1/32 is directly connected, 00:07:07, loopback0
```

It can be seen that leaf1 and leaf2 learn the route of the peer loop port by running the OSPF protocol, which is prepared for leaf1 and leaf2 to establish IBGP neighbors through the loopback port.

Step 4: Configure VXLAN and associate VNID to add ports of leaf1 and leaf2 to VXLAN.

#Configure Leaf1.

```
Leaf1(config)# vxlan 100
Leaf1(config-vxlan-100)#vxlan vnid 100
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit
```

#Configure Leaf2.

```
Leaf2(config)# vxlan 100
Leaf2(config-vxlan-100)#vxlan vnid 100
Leaf2(config-vxlan-100)#exit
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit
```

#View the VXLAN information of Leaf1.

```
Leaf1#show vxlan 100 config

vxlan 100
 vxlan vnid 100
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
```

```
switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk pvid vlan 1
 vxlan 100 encapsulation vlan 2
 exit
```

#View the VXLAN information of Leaf2.

```
Leaf2#show vxlan 100 config

vxlan 100
 vxlan vnid 100
exit

Leaf2#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk pvid vlan 1
 vxlan 100 encapsulation vlan 2
 exit
```

Step 5: Configure the static VXLAN tunnel.

#Configure the NVE interface of Leaf1 and the static header replication members of the corresponding VXLAN.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication peer 20.0.0.1
Leaf1(config-if-nve1)#exit
```

#Configure the NVE interface of Leaf2 and the static header replication members of the corresponding VXLAN.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 20.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication peer 10.0.0.1
Leaf2(config-if-nve1)#exit
```

#View the tunnel information and VXLAN session of Leaf1.

```
Leaf1# show vxlan tunnel
Number of vxlan tunnel: 1
```

```
---- ---------- ------------------ ------------------ ----------
NO.  TunnelID   Source          Destination       State
---- ---------- ------------------ ------------------ ----------
1    32768      10.0.0.1        20.0.0.1          up
```

You can see that the VXLAN tunnel on Leaf1 is successfully established and is the up state.

```
Leaf1#show vxlan session
Number of vxlan session: 1
---- ---------- ---------- ---------- ------------------ ------------------ ----------
NO.  VXLAN-ID   SessionID  TunnelID   Source          Destination       State
---- ---------- ---------- ---------- ------------------ ------------------ ----------
1    100        32768      32768      10.0.0.1        20.0.0.1          up
```

You can see that the VXLAN session with VXLAN-ID 100 on leaf1 successfully binds the tunnel with tunnel ID 32768 and the status is up.

#View the VXLAN information of Leaf2.

```
Leaf2# show vxlan tunnel
Number of vxlan tunnel: 1
---- ---------- ------------------ ------------------ ----------
NO.  TunnelID   Source          Destination       State
---- ---------- ------------------ ------------------ ----------
1    32768      20.0.0.1        10.0.0.1          up
```

You can see that the VXLAN tunnel on Leaf2 is set up successfully and the status is UP.

```
Leaf2#show vxlan session
Number of vxlan session: 1
---- ---------- ---------- ---------- ------------------ ------------------ ----------
NO.  VXLAN-ID   SessionID  TunnelID   Source          Destination       State
---- ---------- ---------- ---------- ------------------ ------------------ ----------
1    100        32768      32768      20.0.0.1        10.0.0.1          up
```

You can see that the VXLAN session with VXLAN-ID 100 on leaf2 successfully binds the tunnel with tunnel ID 32768 and the status is up.

Step 6: Check the result

#VM1 on Server1 pings VM1 on Server2.

```
C:\Documents and Settings\ Server 1> ping 1.0.0.2
Pinging 1.0.0.2 with 32 bytes of data:
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
```

```
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 1.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0m
```

It can be seen that Server1 and server2 can cross the L3 network between leaf1 and leaf2 to realize intercommunication.

13.1.3.2 Configure BGP EVPN VXLAN to Realize L2 Intercommunication

Network Requirements

- Leaf1 and leaf2 serve as VTEP to create the VXLAN instance.
- Leaf1 and Leaf 2 create the BGP EVPN VXLAN tunnel, realizing the intercommunication of Server1 and Server2 in the same segment.

Network Topology

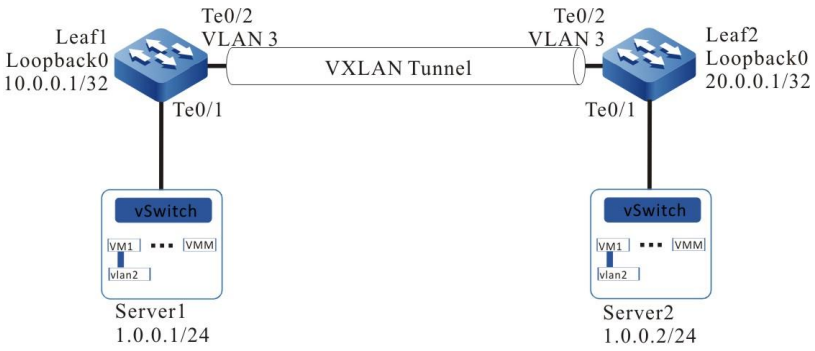


Figure 364 Networking of configuring BGP EVPN VXLAN to realize L2 intercommunication

Configuration Steps

Step 1: Configure VLAN, and add the ports to the corresponding VLAN (omitted).

Step 2: Configure the IP address of the interface.

#Configure Leaf1.

```
Leaf1(config)#interface loopback 0
Leaf1(config-if-loopback0)#ip address 10.0.0.1 255.255.255.255
Leaf1(config-if-loopback0)#exit
Leaf1(config)#interface vlan 3
Leaf1(config-if-vlan3)#ip address 2.0.0.1 255.255.255.0
Leaf1(config-if-vlan3)#exit
```

#Configure Leaf2.

```
Leaf2(config)#interface loopback 0
Leaf2(config-if-loopback0)#ip address 20.0.0.1 255.255.255.255
Leaf2(config-if-loopback0)#exit
Leaf2(config)#interface vlan 3
Leaf2(config-if-vlan3)#ip address 2.0.0.2 255.255.255.0
Leaf2(config-if-vlan3)#exit
```

Step 3: Configure OSPF, making the Loopback route between devices reachable.

#Configure Leaf1.

```
Leaf1#configure terminal
Leaf1(config)#router ospf 100
Leaf1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Leaf1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf1(config-ospf)#exit
```

#Configure Leaf2.

```
Leaf2#configure terminal
Leaf2(config)#router ospf 100
Leaf2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Leaf2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Leaf2(config-ospf)#exit
```

#View the route table of Leaf1.

```
Leaf1#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, 00:05:40, vlan3
C   127.0.0.0/8 is directly connected, 1d:21:38:36, lo0
C   10.0.0.1/32 is directly connected, 00:06:34, loopback0
O   20.0.0.1/32 [110/2] via 2.0.0.2, 00:00:05, vlan3
```

#View the route table of Leaf2.

```
Leaf2#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, 00:06:43, vlan3
C   127.0.0.0/8 is directly connected, 1w3d:03:35:57, lo0
O   10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:36, vlan3
C   20.0.0.1/32 is directly connected, 00:07:07, loopback0
```

We can see that both leaf1 and leaf2 have learned the route of the peer loopback port by running the OSPF protocol.

Step 4: Configure VXLAN and associate VNID, and configure EVPN address family to add ports of leaf1 and leaf2 to VXLAN.

#Configure Leaf1.

```
Leaf1(config)# vxlan 100
Leaf1(config-vxlan-100)#vxlan vnid 100
Leaf1(config-vxlan-100)#address-family evpn
Leaf1(config-vxlan-evpn)#rd 100:1
Leaf1(config-vxlan-evpn)#route-target both 100:1
Leaf1(config-vxlan-evpn)#exit
Leaf1(config-vxlan-100)#exit
Leaf1(config)# interface tengigabitethernet 0/1
Leaf1(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf1(config-if-tengigabitethernet0/1)#exit
```

#Configure Leaf2.

```
Leaf2(config)# vxlan 100
Leaf2(config-vxlan-100)#vxlan vnid 100
Leaf2(config-vxlan-100)#address-family evpn
Leaf2(config-vxlan-evpn)#rd 100:1
Leaf2(config-vxlan-evpn)#route-target both 100:1
Leaf2(config-vxlan-evpn)#exit
Leaf2(config-vxlan-100)#exit
```

```
Leaf2(config)# interface tengigabitethernet 0/1
Leaf2(config-if-tengigabitethernet0/1)# vxlan 100 encapsulation vlan 2
Leaf2(config-if-tengigabitethernet0/1)#exit
```

#View the VXLAN information of Leaf1.

```
Leaf1#show vxlan 100 config

vxlan 100
 vxlan vnid 100
 address-family evpn
  rd 100:1
  route-target import 100:1
  route-target export 100:1
  exit
exit
Leaf1#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk pvid vlan 1
 vxlan 100 encapsulation vlan 2
 exit
```

#View the VXLAN information of Leaf2.

```
Leaf2#show vxlan 100 config
vxlan 100
 vxlan vnid 100
 address-family evpn
  rd 100:1
  route-target import 100:1
  route-target export 100:1
  exit
exit
 Leaf2#show running-config interface te0/1

interface tengigabitethernet0/1
switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk pvid vlan 1
vxlan 100 encapsulation vlan 2
 exit
```

Step 5: Configure BGP.

#Configure Leaf1.

Configure to establish a direct-connected EBGP peer with leaf2, and activate the notification capability under the EBGP address family.

```
Leaf1(config)#router bgp 100
Leaf1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Leaf1(config-bgp)#address-family l2vpn evpn
Leaf1(config-bgp-af)#neighbor 2.0.0.2 activate
Leaf1(config-bgp-af)#exit-address-family
Leaf1(config-bgp)#exit
```

#Configure Leaf2.

Configure to establish a direct-connected EBGP peer with leaf2, and activate the notification capability under the EVPN address family.

```
Leaf2(config)#router bgp 200
Leaf2(config-bgp)#neighbor 2.0.0.1 remote-as 100
Leaf2(config-bgp)#address-family l2vpn evpn
Leaf2(config-bgp-af)#neighbor 2.0.0.1 activate
Leaf2(config-bgp-af)#exit-address-family
Leaf2(config-bgp)#exit
```

#View the BGP EVPN neighbor of Leaf1.

```
Leaf1#show bgp l2vpn evpn summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 5
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      52      50        4    0    0 00:42:18        0

Total number of neighbors 1
```

#View the BGP EVPN neighbor of Leaf2.

```
Leaf2#show bgp l2vpn evpn summary
BGP router identifier 20.0.0.1, local AS number 200
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.0.0.1         4        100      52      53        5    0    0 00:43:20        0
```

```
Total number of neighbors 1
```

We can see that leaf1 and leaf2 have successfully established BGP EVPN neighbors.

Step 6: Configure the NVE interface.

#Configure the NVE interface of Leaf1 and configure the corresponding VXLAN, and use the BGP protocol to build the L2 tunnel dynamically.

```
Leaf1(config)#interface nve 1
Leaf1(config-if-nve1)#source 10.0.0.1
Leaf1(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf1(config-if-nve1)#exit
```

#Configure the NVE interface of Leaf2 and configure the corresponding VXLAN, and use the BGP protocol to build the L2 tunnel dynamically.

```
Leaf2(config)#interface nve 1
Leaf2(config-if-nve1)#source 20.0.0.1
Leaf2(config-if-nve1)#vxlan 100 ingress-replication protocol bgp
Leaf2(config-if-nve1)#exit
```

#View the tunnel information and VXLAN session of Leaf1.

```
Leaf1# show vxlan tunnel
Number of vxlan tunnel: 1
---- ---------- ------------------ ------------------ ----------
NO.  TunnelID   Source          Destination       State
---- ---------- ------------------ ------------------ ----------
1    32768      10.0.0.1        20.0.0.1          up

Leaf1#show vxlan session
Number of vxlan session: 1
---- ---------- ---------- ---------- ------------------ ------------------ ----------
NO.  VXLAN-ID   SessionID  TunnelID   Source          Destination       State
---- ---------- ---------- ---------- ------------------ ------------------ ----------
1    100        32768      32768      10.0.0.1        20.0.0.1          up
```

#View the tunnel information and VXLAN session of Leaf2.

```
Leaf2# show vxlan tunnel
Number of vxlan tunnel: 1
---- ---------- ------------------ ------------------ ----------
NO.  TunnelID   Source          Destination       State
---- ---------- ------------------ ------------------ ----------
```

```
1   32768     20.0.0.1        10.0.0.1        up

Leaf2#show vxlan session
Number of vxlan session: 1
---- ---------- ---------- ---------- ------------------ ------------------ ----------
NO.  VXLAN-ID   SessionID  TunnelID   Source          Destination       State
---- ---------- ---------- ---------- ------------------ ------------------ ----------
1    100        32768      32768      20.0.0.1        10.0.0.1        up
```

From the above information, we can see that the tunnel is up, and the dynamic VXLAN multicast session between Leaf1 and Leaf2 can be established normally. So far, the L2 BUM traffic can be forwarded between Leaf1 and Leaf2.

Step 7: VM1 of Server1 and VM1 od Server ping the different addresses of different segment respectively, and view the VXLAN session of Leaf1 and Leaf2.

#View the VXLAN session of Leaf1.

```
Leaf1#show vxlan session 20.0.0.1
 vxlan session 32768
  state: up
  source IP: 10.0.0.1
  destination IP: 20.0.0.1
  source mac: 0101.7a00.5278
  destination mac: 0101.7a21.81e7
  interface: vlan3
  switchport: tengigabitethernet0/2
  vxlan list: 100
  vxlan unicast list: 100
  vxlan multicast list: 100
```

#View the VXLAN session of Leaf2.

```
Leaf2#show vxlan session 10.0.0.1
 vxlan session 32768
  state: up
  source IP: 20.0.0.1
  destination IP: 10.0.0.1
  source mac: 0101.7a21.81e7
  destination mac: 0101.7a00.5278
  interface: vlan3
  switchport: tengigabitethernet0/2
  vxlan list: 100
```

```
vxlan unicast list: 100
vxlan multicast list: 100
```

It can be seen that dynamic unicast sessions have been established and the L2 unicast traffic can be forwarded.

Step 8: Check the result

#VM1 of Server1 pings VM1 of Server2.

```
C:\Documents and Settings\ Server 1> ping 1.0.0.2

Pinging 1.0.0.2 with 32 bytes of data:

Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255
Reply from 1.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 1.0.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0m
```

You can see that Server1 and Server2 can cross the L3 network between Leaf1 and Leaf2 to realize the intercommunication.

Note

- BGP EVPN supports IBGP and EBGP.
- After BGP enables the EVPN VXLAN capability, the BGP neighbor will be re-set up automatically.

13.2NLB

13.2.1 Overview

NLB is a multi-server cluster load balancing feature developed by Microsoft on Windows Server. When the switch is connected to the NLB server cluster, the NLB

server requires the switch to send the packet whose destination IP address is the IP address of the NLB server cluster to each server in the NLB server cluster.

13.2.2 NLB Function Configuration

Table 1608 NLB function configuration list

Configuration Task	
Configure the NLB function	Configure the static ARP
	Configure the static MAC multi-port

13.2.2.1 Configure NLB

Configuration Condition

None

Configure Static ARP

Table 1609 Configure the static ARP

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Configure the static ARP	arp [vrf *vrf-name*] { *ip-address* | *host-name* } *mac-address*	Mandatory

Note

- When using the NLB function, you need to disable arp smac-check multicast.

Configure Static MAC Multi-Port

After configuring the static forwarding MAC address table entry of multiple egress ports, when the port receives the packet in the corresponding VLAN, it matches the destination MAC address of the packet with the static forwarding MAC address table entry configured in the device. If the matching successfully, the packet will be

forwarded from the specified multiple egress ports. This function can more flexibly send packets to multiple egress ports to achieve multiple forwarding of traffic.

Table 1610 Configure the static forwarding MAC address bound to the multiple egress ports

Step	Command	Description
Enter the global configuration mode	config terminal	-
Configure the static forwarding MAC address bound in the aggregation group	mac-address multiport *mac-address-valu* vlan *vlan-id* interface { *interface-name1* [*to interface-name2*] }	Mandatory By default, do not configure the static forwarding MAC address of multiple egress ports in the device.

13.2.2.2 NLB Monitoring and Maintaining

Table 1611 NLB monitoring and maintaining

Command	Description
show mac-address multiport	Display the MAC multi-port information
show arp	Display the ARP information

13.2.3 NLB Typical Configuration Example

Network Requirements

- After configuring MAC multi-port, static ARP, the packet sent by PC will be sent to all NLB servers.

Network Topology

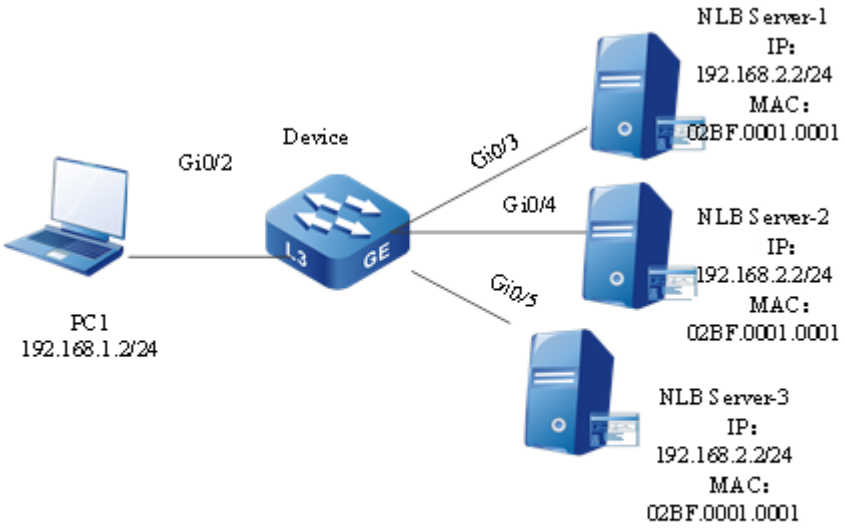


Figure 365 Networking of configuring NLB

Configuration Steps

Step 1: On Device, configure VLAN and port link type and IP address.

#On Device, create VLAN2 and 3.

```
Device#configure terminal
Device(config)#vlan 2,3
```

#Configure the link type of port gigabitethernet0/2 to access, allow the services of VLAN2 to pass, enable interact VLAN2, and configure the IP address to 192.168.1.1/24.

```
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 vlan 2
Device(config-if-vlan2)#ip address 192.168.1.1 255.255.255.0
Device(config-if-vlan2)#exit
```

#Configure the port link type on gigabitethernet 0/3–gigabitethernet 0/5 of Device to Access, allow the services of VLAN2 to pass, enable interface VLAN2, and configure the IP address to 192.168.1.1/24 (omitted).

Step 2: Configure MAC multi-port.

#On Device, configure MAC multi-port, and specify the egress port as gi0/3-gi0/5.

```
Device#configure terminal
Device(config)#mac-address multiport 02BF.1.1 vlan 3 interface gigabitethernet 0/3,0/4,0/5
Device(config)#exit
```

Step 3: Configure the static ARP.

#On Device, configure the static ARP.

```
Device#configure terminal
Device(config)# arp 192.168.2.2 02bf.1.1
Device(config)#exit
```

Step 4: Check the result.

#View the MAC multi-port.

```
Device# show mac-address multiport
mac            vlan          interface
02BF.0001.0001   3             gi0/3-0/5
```

#View ARP.

```
Device# show arp
Protocol  Address        Age (min) Hardware Addr   Type   Interface                Switchport
Internet  192.168.1.1      -       0101.7a6a.011e  ARPA   vlan2                    ---
Internet  192.168.2.1      -       0101.7a6a.011e  ARPA   vlan3                    ---
Internet  192.168.2.2      -       02bf.0001.0001  ARPA   vlan3                    gigabitethernet0/3
Internet  192.168.2.2      -       02bf.0001.0001  ARPA   vlan3                    gigabitethernet0/4
Internet  192.168.2.2      -       02bf.0001.0001  ARPA   vlan3                    gigabitethernet0/5
```

#When accessing the cluster IP of NLB server from PC, each server can receive the packet.